DESARROLLAR UNA PROPUESTA METODÓLOGICA SOBRE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BAJO LA NORMA ISO 27000 EN EL ÁREA DE CONTRATACIÓN DE TRANSMILENIO S.A.

DIDIER ARIEL ARIAS LÓPEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ

2015

DESARROLLAR UNA PROPUESTA SOBRE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BAJO LA NORMA ISO 27000 EN EL ÁREA DE CONTRATACIÓN DE TRANSMILENIO S.A.

MONOGRAFÍA, ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

DIDIER ARIEL ARIAS LÓPEZ

DIRECTOR
MSC. MANUEL ANTONIO SIERRA RODRIGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, 2015

Nota de aceptación:

Firma del presidente del jurado

Firma del jurado

Firma del jurado

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE GRÁFICAS

RESUMEN

En la actualidad los datos son el capital más importante para una empresa, la seguridad informática utiliza diferentes técnicas de seguridad para proteger y fortalecer los sistemas de información de una manera ágil y eficaz y se considera una parte esencial para la seguridad de los datos de una organización. Es de vital importancia tomar todas las medidas necesarias para controlar la transferencia y flujo de la información, desde la instalación de completos antivirus hasta la contratación de operarios y sistemas complejos de protección y vigilancia de los datos. Teniendo en cuenta el notable avance de los métodos de intrusión en los cuales los Hackers cada vez desafían más la seguridad informática ya que logran el entorpecimiento al acceso de miles de personas a sitios web por ataque DDos, consiguen ataques web defacement con protestas religiosas, entre muchos otros que causan perdidas en millones de dólares para todo tipo de organizaciones. Este es el punto de partida para los profesionales de seguridad informática, el cual plantea un futuro incierto, que debe ser asumido con el máximo compromiso para brindar soluciones que minimicen los riesgos presentados, entre las que podemos contar la implementación de herramientas de cifrado, mecanismos de políticas de seguridad y (SGSI) sistemas de gestión de riesgos para proteger la información.

En este trabajo, se hace un reconocimiento de la información relacionada con la seguridad de la información en TRANSMILENIO S.A., esto enfocado en la norma ISO 27000, con el objetivo de desarrollar una propuesta que permita implementar, gestionar y mejorar un SGSI - Sistema de Gestión de Seguridad de la información en la compañía, inicialmente se clasifican, analizan y administran los riesgos buscando las causas y encontrando soluciones, siguiendo los pasos necesarios al momento de implementar el estándar que permitan determinar objetivos de control para los diferentes recursos de la compañía.

Palabras claves: Seguridad informática, SGSI, ISO 27000.

SUMMARY

Currently details are the most important capital for a company; computer security uses different security techniques to protect and strengthen the systems of information in a flexible and effective manner, and is considered an essential part of an organization's data security. It is vital to take all necessary measures to control the transfer and flow of information, since the installation of complete antivirus until the hiring of operators and complex systems of protection and monitoring of the data. Taking into account the remarkable progress of the methods of intrusion in which Hackers increasingly more challenging computer security since they manage the obstacle to the access of thousands of people to web sites for DDos attack, they get attacks web defacement with protest religious, among many others that cause lost millions of dollars for all sorts of organizations. This is the starting point for computer security professionals, which poses an uncertain future, which must be assumed with the utmost commitment to provide solutions that minimize the risks presented, among which we can count the implementation tools of encryption, security policy and (ISMS) mechanisms systems of risk management to protect the information.

In this work, is a recognition of the information related to the security of the information in TRANSMILENIO S.A., this focused on the standard ISO 27000, aiming to develop a proposal that will allow to implement, manage and improve an ISMS in the company, are initially classified, analyze and manage risks for the causes and find solutions, following steps to deploying standard determining control for different resources objectives of the company.

Keywords: Informatic security, ISMS, ISO 27000.

INTRODUCCIÓN

Actualmente y basados en el gran crecimiento de conocimiento e información y la preocupación que existe para administrar eficientemente la misma se requiere la implementación de seguridad a nivel general y específica de los sistemas encargados de albergar datos y almacenar información. De aquí surge la necesidad de mantener todos los sistemas informáticos que manipulan, almacenan y proveen información sensible de las instituciones bajo ciertos estándares y parámetros que permitan garantizar hasta cierto punto la confidencialidad, autenticidad y accesibilidad de la información.

La información es uno de los activos más importantes de cualquier organización por tal razón es imprescindible realizar las tareas necesarias con el fin de preservarla segura y de darle el manejo adecuado buscando que siempre esté disponible y protegida de cualquier posible ataque de carácter particular tanto interno como externo.

El mundo actual vive cambios cada segundo, el crecimiento acelerado de la tecnología, el aumento de la competencia a través del internet, entre otros son factores que influyen en las decisiones de las empresas en el momento de invertir, debido a esto pasan por alto temas sensibles en cuanto a la seguridad de la información por cuestiones económicas o por el desconocimiento de normas y leyes aplicables.

Todas las personas de la organización deben aportar lo necesario para la adopción de un SGSI - Sistema de Gestión de Seguridad de la información, esto en la búsqueda de lograr una compañía exitosa, prolongar su rendimiento y consolidar la seguridad de la información.

La siguiente propuesta constituye una base de referencia para el desarrollo de los sistemas de información corporativos y la implementación de las políticas informáticas que respondan y ayuden al cumplimiento de los objetivos estratégicos de la Entidad.

1. MARCO CONCEPTUAL

1.1. JUSTIFICACIÓN

El desarrollo de la propuesta sobre un SGSI – Sistema de Gestión de Seguridad de la información en TRANSMILENIO S.A. buscará minimizar los riesgos físicos y lógicos de los activos de información que afecten la productividad de la compañía debido a falencias que pueden comprometer la confidencialidad, disponibilidad e integridad de la información o de algún activo informático.

Los procesos informáticos en TRANSMILENIO S.A. deben contar con alta disponibilidad, con el fin de no afectar las tareas ni el alto flujo de operaciones que posee la compañía. La no disponibilidad de los sistemas de información en cualquier área retardará las actividades diarias de la empresa, lo que ocasionaría una imagen negativa entre los usuarios internos y externos.

Mediante la inclusión de la norma ISO 27000 se pretende brindar una solución a diversos aspectos que cubre la seguridad informática en la compañía, por medio de una metodología de trabajo se ofrece un diagnóstico claro de la situación actual, estableciendo debilidades y fortalezas, que posteriormente serán ajustadas y corregidas, para generar un valor agregado a la organización logrando altos niveles de competitividad, rentabilidad e imagen corporativa, además del respaldo que brinda la norma en el ámbito nacional e internacional.

1.2. DEFINICIÓN DEL PROBLEMA

1.2.1.1. DESCRIPCIÓN DEL PROBLEMA

TRANSMILENIO S.A. es una Entidad del Distrito Capital que ha construido una imagen de ciudad moderna y es un ejemplo a nivel nacional e internacional siendo reconocida y aceptada por todos sus habitantes al prestar un servicio de transporte rápido eficiente y seguro. Es indudable que la fortaleza tecnológica en que esta soportada la operación y administración del sistema de transporte debe evolucionar hacia la satisfacción de los requerimientos de los usuarios.

Es evidente el crecimiento en las operaciones de la compañía no solo en sus sistemas de información sino también en todas las herramientas tecnológicas de apoyo, lo que ha generado un incremento importante en el volumen de información y una necesidad de transferencia de datos entre la organización y terceras partes o ciudadanos en general. Es por esto que TRANSMILENIO S.A. está en la obligación de custodiar, proteger y dar un correcto uso a la información que sirve de apoyo a los procesos de negocio o sean estratégicos para su gestión.

Es claro que para una empresa de tal magnitud la información es un elemento vital, es aquí donde encontramos que existen procesos con amenazas constantes en materia informática lo cual evidencia que existen falencias en temas de seguridad informática por lo cual se deben adelantar proyectos que apunten a fortalecer las condiciones de seguridad de la información en la entidad.

TRANSMILENIO S.A. necesita proteger y reforzar su activo más valioso (la información). Este problema se ve agravado, debido a que los datos de la compañía y su complejidad de análisis crecen de manera exponencial, razón por la cual se pretende establecer una metodología de seguridad que asegure la confidencialidad, integridad y disponibilidad de la información, lo cual brindara fiabilidad y seguridad en las todas las operaciones en que se utilicen herramientas tecnológicas, todo esto es el punto de central en el que se fundamenta el éxito de la compañía.

1.2.1.2. FORMULACIÓN DEL PROBLEMA

¿Cómo proteger los sistemas de información de los riesgos físicos y lógicos relacionados con la utilización de las herramientas tecnológicas en el área de contratación de TRANSMILENIO S.A.?.

1.3. OBJETIVOS

Objetivo General

Proponer un Sistema de Gestión de seguridad de la información basado en la norma ISO 27000 para optimizar los procedimientos de utilización y protección de la información en el área de contratación de TRANSMILENIO S.A.

Objetivos específicos

Revisar el estado del arte en cuanto a la seguridad de la información en TRANSMILENIO S.A.

Realizar un análisis y evaluación de riesgos físicos y lógicos existentes en el área de contratación y establecer medidas que minimicen sus efectos sobre los activos de TI. (Tecnología de la información).

Definir políticas de seguridad que permitan asegurar la información en el área de Contratación.

Elaborar una propuesta que permita el desarrollo de un SGSI - Sistema de Gestión de Seguridad de la información en el área de contratación.

1.4. MARCO TEORICO

La serie ISO/IEC 27000 (ISO, 2015b) consta de las normas de seguridad de información publicadas por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC). La serie está diseñada para dar recomendaciones de buenas prácticas sobre la gestión de seguridad de la información, incluidos los riesgos y los controles en el marco de un Sistema de Gestión de la Información general de Seguridad (SGSI), de una manera similar a los sistemas de gestión para el aseguramiento de la calidad (ISO 9000) (ISO, 2015c) y la protección del medio ambiente (ISO 14000) (ISO, 2015a).

A principios de la década de los 90, el Departamento de Comercio e Industria del Reino Unido Department of Trade and Industry's (DTI) emprendió el desarrollo de una norma, para el establecimiento de un conjunto de criterios de evaluación de seguridad reconocidas internacionalmente y un sistema de evaluación y certificación asociada con el fin de salvaguardar y reglamentar la gestión de la seguridad en las compañías, esto como respuesta a los requerimientos de los sectores productivos y el estado para implantar una estructura común de seguridad de la Información. La primera norma aprobada oficialmente en 1995 fue la (BS 7799:1995) (ISO 27000.es, 2013) y aparece como un código de buenas prácticas para la gestión de seguridad de la información.

Una segunda parte BS7799-2: 1998 fue introducida en febrero de 1998 después de una extensa revisión y el período de consulta pública, que se inició en noviembre de 1997, la primera revisión de la norma, BS7799: 1999 fue publicada en abril de 1999 la parte 1 de la norma fue propuesta como un estándar ISO en octubre de 1999, y publicada con modificaciones menores como la ISO / IEC 17799: 2000 el 1 de diciembre de 2000, BS 7799-2: 2002 fue lanzado oficialmente el 5 de septiembre de 2002. En la que se establecían el alcance de la norma y los requisitos para la implementación de un SGSI certificable. En el año 2005 se publica la norma ISO/IEC 27001:2005 e ISO/IEC17799:2005: Aparece el estándar ISO 27001 como norma internacional certificable y se revisa la ISO 17799 dando lugar a la ISO 27001:2005 (ISO/IEC, 2005) que reemplaza a la norma BS 7799-2 (ISO 27000.es, 2013) .

Sobre ISO / IEC 17799: 2005, como resultado del ciclo regular de actualización de las normas ISO. El cambio más significativo está en el diseño de los controles, que ahora distingue claramente entre los requisitos, la guía de implementación y más información sobre definiciones y términos. Hay también una cierta racionalización, con la adición de algunos nuevos controles y los controles existentes mejor explicados. La norma revisada ahora cuenta con 11 secciones principales y 133 controles, Hay dos nuevas secciones principales: la primera pone los controles en un marco contextual más fuerte en la evaluación y tratamiento de los riesgos, la otra hace la separación de los controles relativos a la gestión de incidentes.

En 2005, BS 7799-2, finalmente entró en el mecanismo de vía rápida ISO y surgió el 14 de octubre de 2005 como ISO / IEC 27001: 2005. Hay mucha similitud entre las dos normas y las diferencias son relativamente insignificantes. La primera diferencia que es digna de mención es la adopción de la norma ISO / IEC 17799: 2005 en la base de la SOA (Statement of Applicability). La segunda es la introducción de un nuevo requisito métrico del SGSI y la necesidad de medir la eficacia de los controles de seguridad de la información, esto abarca el análisis y gestión de riesgo**.** El objetivo básico de la norma ISO 27001 es ayudar a establecer y mantener un sistema eficaz de gestión de la información, utilizando un enfoque de mejora continua que administre la seguridad de los sistemas de información.

El 1 de julio de 2007, una Rectificación Técnica (N º 1) fue publicada una nueva versión de la ISO/IEC 27001:2007 para reemplazar a la norma 17799 ISO / IEC: 2005 con lo que el nombre del Código de buenas prácticas pasa a ser la ISO 27002:2005.

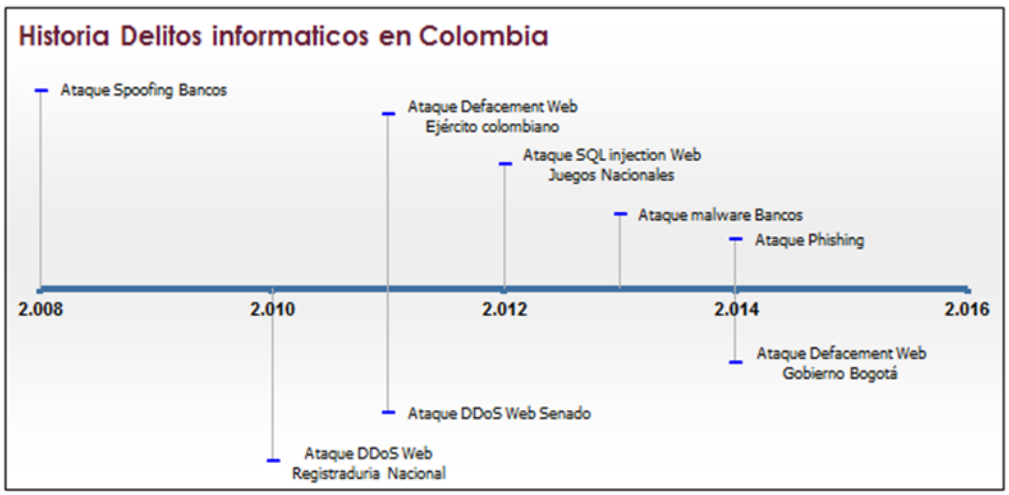
El 25 de septiembre de 2013 se publicaron nuevas ediciones de la norma ISO / IEC 27001 e ISO / IEC 27002, la última revisión de la norma titulada ISO 27001: 2013 se publicó. Sobre la base de la nueva estructura de alto nivel Anexo SL de ISO, que está diseñado para ser más compatible con otras normas de sistemas de gestión. La actualización también tiene en cuenta el cambiante mundo de la seguridad de la información, donde la delincuencia cibernética, la computación en nube y los teléfonos inteligentes han cambiado el panorama considerablemente. Más que nunca, se reconoce como el mejor estándar de práctica para demostrar las credenciales de seguridad de la información.

La nueva edición de la norma ISO / IEC 27001 se ve radicalmente diferente a la edición de 2005. Esto se debe a que sigue la nueva estructura estándar para todas las normas de sistemas de gestión. Sin embargo, la filosofía básica y la intención no han cambiado. Muchos conceptos se han generalizado, con mejoras sutiles en la forma en que se especifican los requisitos, pero con más claridad en la definición de los controles por el proceso de tratamiento de riesgos. En general, en la actualidad hay 114 controles identificados y organizados bajo 14 títulos principales.

1.5. MARCO LEGAL

La Gráfica 1, representa los delitos informáticos en Colombia desde 2008 hasta 2014.

Gráfica 1 Historia Delitos Informáticos en Colombia



Fuente: Autoría propia

DELITOS INFORMÁTICOS Y LEYES APLICABLES

La Tabla 1 describe diferentes tipos de ataques informáticos, la descripción y las leyes colombianas aplicables.

Tabla 1 Delitos Informáticos y Leyes Aplicables

N°	Tipo de ataque	Descripción	Leyes aplicables
1	Spoofing	Delincuentes actuaban en Bogotá, donde desde salas de Internet creaban cuentas de ahorro y generaban sobregiros millonarios. (13/08/2008)	Ley 1273 de 2009 Art: 269A: Acceso abusivo a un sistema informático Art: 269D: Daño Informático Art: 269I: Hurto por medios informáticos y semejantes Art: 269J: Transferencia no consentida de activos
2	Denegación de servicios	Ataque de Hackers a la registraduría (14/03/2010).	Ley 1273 de 2009 Art: 269B: obstaculización ilegítima

			del sistema informático o red de telecomunicación
3	Defacement	Ataque de defacer a la página del Ejército colombiano (05/09/2011)	Ley 1273 de 2009: Art: 269A: Acceso abusivo a un sistema informático Art: 269D: Daño Informático.
4	Denegación de servicios	Ataque de Hackers a la página del Senado colombiano (21/09/2011)	Ley 1273 de 2009 Art: 269B: obstaculización ilegítima del sistema informático o red de telecomunicación
5	SQL injection	Ataque de Hacker la página oficial de los Juegos Nacionales (10/11/2012)	Ley 1273 de 2009: Art: 269A: Acceso abusivo a un sistema informático Art: 269D: Daño Informático.
6	Código malicioso	Banda desarrollaba programas informáticos con capacidad para vulnerar los servicios de la banca virtual (12/11/2013)	Ley 1273 de 2009: Art: 269A: Acceso abusivo a un sistema informático Art: 269E: Uso de software malicioso
7	Defacement	Ataque de defacer a la página GobiernoBogota.gov.co (21/03/2014)	Ley 1273 de 2009: Art: 269A: Acceso abusivo a un sistema informático Art: 269D: Daño Informático.
8	Phishing, spamming	Utilizan falsos correos de Avianca y la Dian para instalar programa en computadores colombianos (12/01/2014)	Ley 1273 de 2009: Art: 269G: Suplantación de sitios web para capturar datos personales.

Fuente: Autoría propia

1.6. MARCO CONTEXTUAL

Seguridad de la información

La seguridad de la información busca la protección de los principios básicos de confidencialidad, integridad y disponibilidad de la misma y de los sistemas involucrados en su tratamiento. Estos conceptos fundamentales se definen como:

Confidencialidad: Asegura el acceso a la información solamente a las personas autorizadas.

Integridad: Busca evitar alteraciones no autorizadas en los datos.

Disponibilidad: Procura brindar el acceso a la información y a los sistemas mediante usuarios autorizados en el momento requerido.

Que es un Sistema de Gestión de Seguridad de la Información (SGSI)?

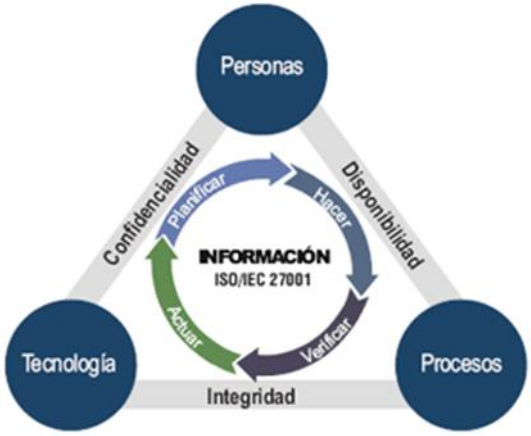
"Es un proceso sistemático, documentado y conocido por toda la Organización, construido desde un enfoque del riesgo empresarial, para garantizar que la Seguridad de la Información sea gestionada correctamente" (ISO 27000.es, 2013).

Un SGSI - Sistema de Gestión de Seguridad de la información busca en una organización el diseño, la implantación y el mantenimiento de una serie políticas con el fin de administrar eficientemente la seguridad de la información, pretendiendo asegurar la confidencialidad, integridad y disponibilidad de los activos de información, utilizando mejores prácticas para reducir los riesgos a los que actualmente están expuestas las organizaciones.

El SGSI - Sistema de Gestión de Seguridad de la información debe procurar la eficiencia de la seguridad de la información durante un largo periodo, además debe adaptarse a los cambios internos de la organización y a los externos del entorno.

La Gráfica 2 visualiza el modelo PDCA.

Gráfica 2 ISO/IEC 27001



Fuente: (ALIGNET, 2009)

La implantación de un SGSI - Sistema de Gestión de Seguridad de la información permitirá a la compañía establecer un proceso de mejora continua en el tema a través del seguimiento de un modelo PDCA (Planificar, Hacer, Verificar, Actuar), con unas responsabilidades claras y el compromiso manifiesto por parte del Gerente y demás directivos en la empresa.

Un SGSI - Sistema de Gestión de Seguridad de la información prepara a las empresas ante imprevistos de una manera rápida y eficiente, analiza los riesgos y los da conocer, establece medidas de seguridad y dispone de controles que evalúan las medidas. Todo de una manera documental que permitirá que el sistema se pueda asumir rápidamente por nuevas personas.

Serie ISO/IEC 27000

Estándares que proporcionan un marco de referencia para la gestión de la seguridad de la información.

27000 Términos y Definiciones usados en toda la Serie 27000.

27001 Requisitos de un SGSI.

27002 Objetivos de Control y Controles de Seguridad de la Información.

27003 Guía para implantar un SGSI según el Modelo PDCA y los requerimientos de sus diferentes fases.

27004 Métricas y Técnicas de Medida para determinar la eficacia de un

SGSI y de los Controles de Seguridad aplicados.

27005 Directrices para la Gestión de Riesgos en la Seguridad de la Información.

27006 Requisitos para la Acreditación de Entidades de Auditoría y Certificación de SGSI.

2. ASPECTOS METODOLOGICOS

Este proyecto utiliza una investigación descriptiva ya que detalla y especifica los componentes de la investigación lo cual permitió comprobar las vulnerabilidades de seguridad de la información en el área de Contratación de TRANSMILENIO S.A.

2.1. POBLACIÓN:

Funcionarios del área de contratación de TRANSMILENIO S.A.

2.2. MUESTRA

100% de los funcionarios del área de contratación de TRANSMILENIO S.A.

2.3. TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

- **Encuestas:** Las preguntas realizadas a los profesionales del área de contratación se basaron en información general sobre el manejo y uso de la información y las medidas de seguridad de la información en la Entidad.
- **Entrevistas:** Con el fin de recolectar información de vital importancia para el proyecto se utilizaron entrevistas sobre seguridad de la información y sobre el cumplimiento de algunos requisitos de la norma ISO 27000 realizadas a algunos de los profesionales de la Dirección de Tics y al personal de soporte técnico de la Entidad.
- **Observación:** Se realizó por parte del investigador la observación de las prácticas comunes de los usuarios del área de contratación en el manejo de los activos de información.
- **Procedimientos internos**:: Entre otros se encuentran el Sistema integrado de gestión, Políticas de seguridad, reportes de auditoria, y contratos.

2.4. VARIABLES:

Activos, amenazas, vulnerabilidades, usuarios.

2.5. DESCRIPCIÓN DE LA METODOLOGIA

Para realizar el diseño de un SGSI - Sistema de Gestión de Seguridad de la información, consideramos algunos de los puntos esenciales a tener en cuenta.

2.5.1.1. PROGRAMACIÓN DEL PROYECTO CON LA COORDINACIÓN DEL ÁREA DE CONTRATACIÓN DE TRANSMILENIO S.A.

Este proceso permitió la planificación de las actividades y brindo claridad a los directivos sobre la importancia del proyecto a implantar y la necesidad del apoyo del personal del área, factor de suma importancia para dar inicio a la fase de levantamiento de información.

2.5.1.2. DEFINIR EL ALCANCE DEL PROYECTO

Debido a la complejidad de la implantación de un SGSI bajo la norma ISO 27000, es recomendable definir el alcance del proyecto en el área de contratación de TRANSMILENIO S.A.

- Control de activos: realizar un inventario de los activos para tener un control riguroso sobre estos.
- Seguridad de los recursos humanos: asegurar que los usuarios, comprenden sus responsabilidades y son capaces de realizar sus funciones, teniendo en cuenta los riesgos que existen (hurto, fraude o uso inadecuado de las instalaciones).
- Análisis de vulnerabilidades: Aplicar procedimientos que protejan el acceso a la información.

2.5.1.3. GESTIÓN Y TRATAMIENTO DE RIESGOS

En este proceso inicialmente se determinan los riesgos existentes en la organización seguidamente se establecen las medidas que permiten controlar, minimizar o eliminar los riesgos que afectan los activos de la compañía.

2.5.1.4. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Se establece un documento que define pautas generales a través de un conjunto de políticas y procedimientos para la protección de los activos de la información de TRANSMILENIO S.A. Las políticas de seguridad proveen la base para la implementación de controles de seguridad que reducen los riesgos y vulnerabilidades del sistema.

2.6. RECURSOS DISPONIBLES

La tabla 2 muestra los recursos disponibles para el desarrollo del proyecto.

Tabla 2 Recursos Disponibles

<table>
<tr><th>Recurso Físico</th><th>Recurso Humano</th><th>Recurso Técnico</th><th>Recursos Financieros</th></tr>
<tr><td>Equipo Portátil (1).</td><td>Ingeniero de Sistemas con Estudios en Seguridad Informática (1).</td><td>Herramientas de software libre (Backtrack, Caine, Wireshark, Clonezilla, Virtual Box, etc.).</td><td rowspan="6">Debido a la naturaleza este proyecto de investigación (Investigativa y académica) no ocasionara gastos ya que el especialista de seguridad informática utilizara software libre, herramientas de cómputo propias, además de los recursos técnicos que brinda la compañía para las labores diarias.</td></tr>
<tr><td>Computador de escritorio.</td><td>Funcionarios del área de contratación</td><td>Encuestas presenciales</td></tr>
<tr><td>Conexiones inalámbricas.</td><td rowspan="4">Funcionarios del área de Tics</td><td rowspan="4">Herramientas de Software (Navegadores, suite de ofimática, visor de PDF, email, etc.</td></tr>
<tr><td>Dispositivos USB.</td></tr>
<tr><td>Tablet (1).</td></tr>
<tr><td>Red LAN.</td></tr>
</table>

Fuente: Autoría propia

3. ESTADO DEL ARTE

La cantidad de delitos informáticos en la actualidad ha incrementado ostensiblemente, estadísticasobtenidas de la National Vulnerability Database del gobierno de Estados Unidos muestran el aumento considerable de vulnerabilidades en los últimos tres años, lo cual ha sido aprovechado por individuos para causar daños a personas y empresas, es evidente que el costo de eliminar una vulnerabilidad es mucho mayor al costo de prevenirla utilizando un SGSI - Sistema de Gestión de Seguridad de la información,

A continuación se presenta el resultado del trabajo de investigación sobre los avances de la Dirección de Tics en la implementación de la Seguridad de la información durante los últimos 5 años en TRANSMILENIO S.A., la información aquí presentada, fue obtenida a través de una amplia revisión documental, aquí se presenta y analiza la información relacionada con la implementación de un SGSI - Sistema de Gestión de Seguridad de la información. Logrando exponer los últimos avances sobre el área de la Seguridad de la Información, en la investigación realizada se evidencian conceptos fundamentales para la Entidad como el SIG (Sistema Integrado de Gestión) sus políticas y objetivos, que son la base para la construcción de un SGSI, a su vez se presenta la estructura de la compañía, resaltando la misión, visión y los objetivos organizacionales, además se despliega la inversión realizada por la entidad en Seguridad de la información, finalmente se expone la Normativa relacionada con un SGSI - Sistema de Gestión de Seguridad de la información en el Distrito y la Entidad.

3.1. SISTEMA INTEGRADO DE GESTIÓN DE TRANSMILENIO S.A.

TRANSMILENIO S.A. como ente gestor del Sistema Integrado de Transporte Público y que tiene a su cargo la planeación estructural del Sistema y la definición del régimen técnico que regula la operación, gestión y control de la operación troncal y alimentadoras y la supervisión de todas las zonas del sistema, define y estructura su Sistema Integrado de Gestión, como herramienta de gestión y soporte de cada a cada una de las operaciones adelantadas en la entidad para el cumplimiento de su objeto social y corporativo.

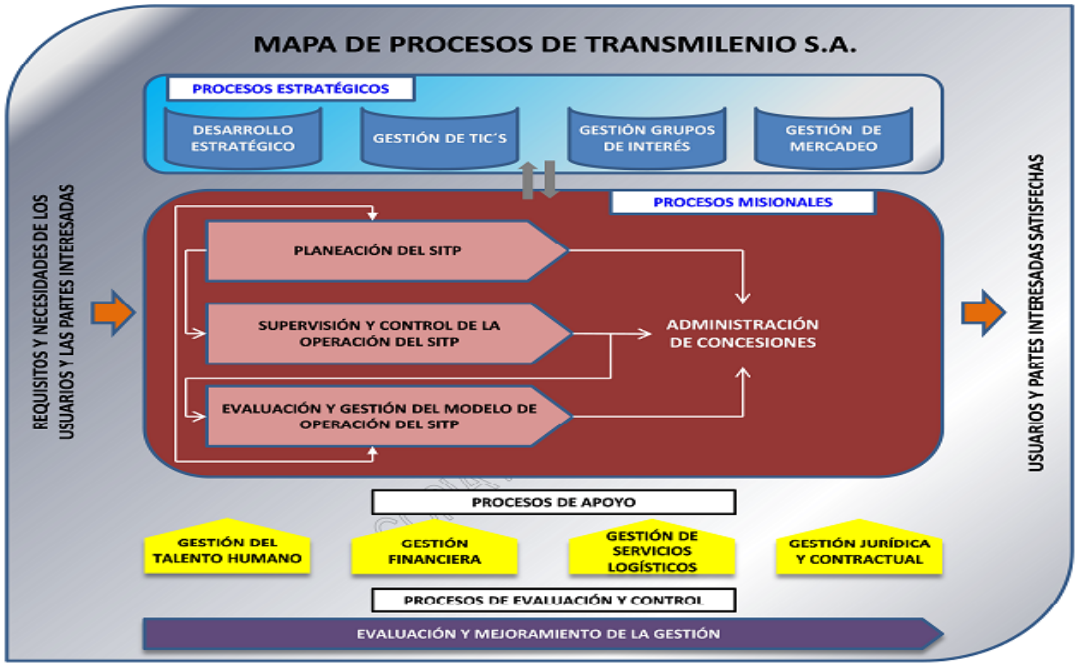
TRANSMILENIO S.A. desarrolla su misión a través de los procesos estratégicos, misionales, de apoyo y de evaluación y control, lo que permite ejecutar de manera eficaz sus funciones y generar mayores sinergias e interacciones eficaces entre procesos y colaboradores para el logro de los objetivos de la entidad.

La siguiente gráfica muestra el MAPA DE PROCESOS de la entidad. Cada uno de estos procesos está constituido por una serie de subprocesos que a su vez se encuentran caracterizados a través de un ciclo PHVA (Planificar – Hacer – Verificar - Actuar) y sus diferentes componentes:

- Objetivo Principal y Responsable de su gestión
- Entradas o Insumos y sus Proveedores
- Salidas y Clientes (Entendido este concepto desde el punto de vista interno y externo)
- Requisitos normativos y legales aplicables
- Recursos asociados
- Referencia a los documentos e Indicadores aplicables

La Gráfica 3 visualiza el Mapa de procesos de TRANSMIELENIO S.A.

Gráfica 3 Mapa de procesos TMSA



Fuente: (TRANSMILENIO S.A., 2015)

3.2. POLÍTICA Y OBJETIVOS DEL SISTEMA INTEGRADO DE GESTIÓN

La Política Integrada de Gestión, establece las directrices a seguir a respecto a la calidad (SGC), el medio ambiente (SGA) y la seguridad y salud de los actores del Sistema TransMilenio (S&SO). De igual forma y de manera implícita establece los lineamientos a seguir respecto de los demás subsistemas componentes del Sistema Integrado de Gestión: Gestión Documental y Archivo (SIGA), Gestión de la Seguridad de la Información (SGSI), Responsabilidad Social (SRS) y Control Interno (SCI). (TRANSMILENIO S.A., 2012)

3.3. ESTRUCTURA ORGANIZACIONAL TRANSMILENIO S.A

Según el Acuerdo 002 de 2011 de la Junta Directiva de TRANSMILENIO S.A., la organización interna de la empresa está estructurada en tres ámbitos de gestión: Alta Gerencia, Gerencia de la Integración, Dirección y Control de la Operación:

La Gráfica 4 deja ver la estructura organizacional de TRANSMILENIO S.A.

Gráfica 4 Estructura Organizacional TMSA

Fuente: (TRANSMILENIO S.A., 2013b)

3.4. FUNDAMENTOS ESTRATÉGICOS TRANSMILENIO S.A

3.4.1.1. MISIÓN

Satisfacer la necesidad de transporte público de los usuarios del Distrito Capital y su área de influencia, con estándares de calidad, eficiencia y sostenibilidad, mediante la planeación, gestión, implantación y control de la operación de un sistema integrado de transporte público urbano de pasajeros, que opere bajo un esquema público-privado, que contribuya a una mayor competitividad de la ciudad y al mejoramiento de la calidad de vida de los habitantes. (TRANSMILENIO S.A., 2013a)

3.4.1.2. VISIÓN

Ser la organización que administra la operación del Sistema Integrado de Transporte Público, para atender con calidad, eficiencia y sostenibilidad la demanda de transporte público en el Distrito Capital y su área de influencia, que contribuya al

desarrollo económico y social mediante la acción conjunta de lo público y lo privado, constituyéndose en un modelo a seguir a nivel nacional e internacional (TRANSMILENIO S.A., 2013c).

3.5. OBJETIVOS ORGANIZACIONALES

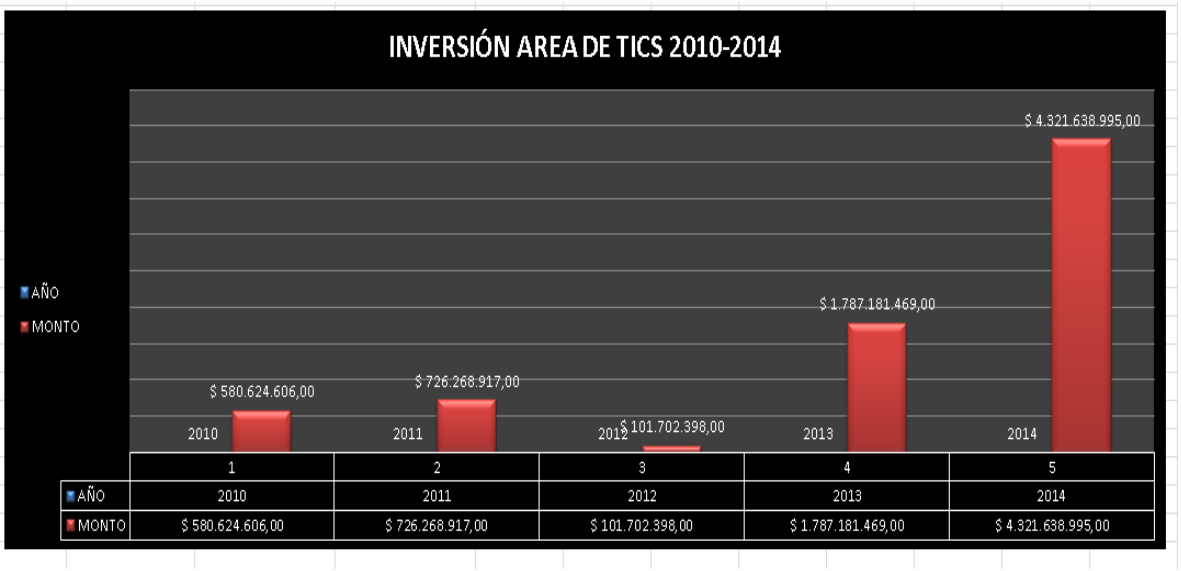
La Gráfica 5 nos permite visualizar los objetivos organizacionales de la compañía.

Gráfica 5 Objetivos Organizacionales TRANSMILENIO S.A

OBJETIVO	Objetivo Estratégico
1.Contribuir a la movilidad de los usuarios del transporte público en el Distrito Capital, con la operación de un sistema eficiente	1.1. Implementar, integrar y optimizar sistemas de control de la operación en tiempo real.
	1.2. Establecer mecanismos de participación para el mejoramiento continuo del servicio con los diferentes actores del Sistema Integrado de Transporte Público.
2. Mejorar la calidad en la prestación del servicio del Sistema Integrado de Transporte Público.	2.1. Desarrollar una cultura integral de servicio al usuario
	2.2. Desarrollar y fortalecer los canales de comunicación con los usuarios.
3. Buscar mecanismos que contribuyan a la sostenibilidad del Sistema Integrado de Transporte Público	3.1. Procurar la sostenibilidad financiera de los agentes del Sistema.
	3.2. Procurar ingresos comerciales para TRANSMILENIO S.A.
4. Optimizar la gestión empresarial de TRANSMILENIO S.A.	4.1. Implementar mecanismos para lograr la adecuada gestión de la información de la entidad TMSA.
	4.2. Diseñar y mantener un esquema de control para realizar seguimiento permanente a la gestión contractual de la empresa.

Fuente: TRANSMILENIO S.A

Gráfica 6 Inversión Área Tics 2010-2014



	1	2	3	4	5
AÑO	2010	2011	2012	2013	2014
MONTO	$ 580.624.606,00	$ 726.268.917,00	$ 101.702.398,00	$ 1.787.181.469,00	$ 4.321.638.995,00

Fuente: Autoría Propia

Es evidente que el incremento en las operaciones de la empresa no solo en sus sistemas de información misionales sino también en todas las herramientas tecnológicas de apoyo, han generado un aumento significativo en el volumen de información y una necesidad latente en la transmisión de datos entre la Entidad y terceras partes o ciudadanos en general. Es por esto que la organización está en la obligación de custodiar, proteger y darle un correcto tratamiento a los datos que sirvan de apoyo a los procesos de negocios o sean estratégicos para su gestión.

Haciendo un poco de historia a finales del 2008 se adelantó un proyecto que tenía como propósito la Evaluación y Análisis del Riesgo Informático de TRANSMILENIO S.A. y el Diseño de la Estrategia de recuperación de la Infraestructura Tecnológica para TRANSMILENIO S.A.; en similar sentido el proceso de revisoría interna efectuó la Evaluación de controles generales de tecnología de información. Los resultados de ambos procesos apuntaron a fortalecer las condiciones de seguridad de la información en la Entidad.

En el plan de acción 2009 de la entidad avaló la inversión inicial en esta línea de actuación. La subgerencia general y la Oficina Asesora jurídica fueron comisionadas por la Gerencia general para liderar el proceso.

Como consecuencia de esto en el año 2010 se realizó un análisis de vulnerabilidades sobre la seguridad de la infraestructura tecnológica de TRANSMILENIO S.A. que trajo como resultado los siguientes componentes:

1. Definición y documentación de la Política, directrices, normas y procedimientos de seguridad de la información para TRANSMILENIO S.A.

2. Definición de la organización para seguridad de la información en TRANSMILENIO S.A.

3. Evaluación, concientización y promoción de la cultura de seguridad de la Información en TRANSMILENIO S.A.

4. Provisión, instalación y configuración de hardware de seguridad perimetral tipo UTM (firewalls-hardware.com, 2015) para la implementación de medidas de protección ante vulnerabilidades internas y externas.

En el año 2011 se adquieren las licencias de un antivirus para los equipos de cómputo, los servidores de datos y la información allí almacenada, ya que la falta de este importante software hace que la red en general sea altamente vulnerable a posibles ataques externos que puedan incurrir en pérdidas importantes de información para TRANSMILENIO S.A., que afectarían el correcto desempeño de las tareas de los funcionarios.

El producto adquirido fue la actualización de trescientas (300) licencias de antivirus Kaspersky Enterprise Space Security (Insight Technology Solutions S.L., 2015), adquisición de doscientas (200) licencias de antivirus Kaspersky Enterprise Space Security, para todos los equipos de cómputo y servidores, incluyendo un servidor de MS Exchange 2010. Este licenciamiento fue obtenido por tres (3) años.

El objetivo de este antivirus contemplo:

- Detectar y eliminar todo tipo de virus, spyware, troyanos, adware, phishing, rootkits, hacker, spam, dialer y otro tipo de amenazas informáticas.
-
  Permitir trabajar sobre plataformas: Windows 2000, XP, Vista y Servers.
-
  Ofrecer el manejo centralizado en las estaciones de trabajo y servidores, incrementando la efectividad en la protección.
-
  Generar automáticamente reportes de las actividades.

- La exploración del equipo puede ser ejecutada en segundo plano sin consumir mucho recurso de máquina.

- Monitorear los cambios en archivos ejecutables para detectar intrusiones. Ejecutarse mínimo cada día y de forma automática, las actualizaciones del producto.

- Permitir un escaneo rápido y seguro.

- Actualizar las firmas de virus y el producto desde una máquina de red local, facilitando la actualización local, sobre las maquinas que no cuenten con conexión a internet.

- Al detectarse un virus, envía mensajes detallados sobre el mismo.

- Adicionalmente se debe tener un antivirus para el servidor de correo Exchange.

- En el año 2012 no hubo inversión por parte de la entidad en seguridad de la información.

- En el año 2013 el SITP, ha ido creciendo, han aumentado el número de sistemas de información, el número de servidores y de usuarios de estos sistemas y en gran magnitud ha aumentado el volumen de transacciones y de datos e información almacenada.

En razón a este crecimiento y en cumplimiento con la norma ISO 27001 (“INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Information security management systems — Overview and,” 2014), en el año 2011 bajo el contrato CT0173-11, se adecuó y remodeló la infraestructura del Centro de Cómputo Administrativo de TRANSMILENIO S.A., con excelentes prestaciones de red de datos, seguridad y capacidad de crecimiento a futuro.

No obstante, en el año 2012 se expidió el estándar internacional ISO 22301 (BSIGROUP, 2015) "Gestión de Continuidad del Negocio", que ayuda a las empresas a mejorar su capacidad de recuperar y restaurar sus funciones críticas parcial o completamente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre. Es entonces, esencial para TRANSMILENIO S.A., anticiparse a los eventos no deseados y diseñar e implantar planes de contingencia efectivos para mantener la actividad del negocio, sin importar qué pueda ocurrir.

En este sentido, y en cumplimiento de la norma ISO 22301, TRANSMILENIO S.A., adquiere una Solución Integral Tecnológica, alterna, con especificaciones internacionales ANSI/TIA-942 (C3comunicaciones.es, 2014) (Telecommunications Infrastructure Standard for Data Centers) tipo TIER IV (CATRIAN, 2014), que permita la alta disponibilidad del Centro de Computo Administrativo de TRANSMILENIO S.A., como plan de contingencia y continuidad del negocio, según la normatividad vigente aplicable.

En el año 2014 TRANSMILENIO S.A., cuenta con una infraestructura de equipos activos, compuesta por FIREWALL marca SonicWall NSA 3500 (SONICWALL, 2011), un core Allied TelesIs BLADE X908 (Allied Telesis, 2015b) y switches de frontera marca Alied TelesIs AT8000GS/24 POE (Allied Telesis, 2015a). Con el propósito de asegurar la utilización adecuada de la tecnología y a fin de reducir importantes riesgos para la confiabilidad, integridad y la disponibilidad de la información institucional, así como el aseguramiento de la prestación de sus servicios.

De acuerdo con lo anterior y con el fin de mantener en óptimas condiciones de funcionamiento tanto el software como los equipos que están instalados, así como de actualizar la plataforma tecnológica, TRANSMILENIO S.A., adquiere la siguiente infraestructura con el objetivo de fortalecer las redes de telecomunicaciones.

La Gráfica 7 describe la infraestructura de seguridad de TRANSMILENIO S.A.

Gráfica 7 Descripción infraestructura de seguridad

IT	DESCRIPCION
SOLUCIÓN DE SEGURIDAD UTM CON NSA 3600	
1	Un (1) Dell SonicWALL Network Security Appliance NSA 3600 TotalSecure(1 Yr) Incluye licencias y Soporte DELL 7x 24 por un año.
SOLUCIÓN NSA 3600 HA	
2	Un (1) Dell SonicWALL NSA 3600 High Availability (HA) Unit
3	Stateful HA upgrade For NSA 3500 and NSA 3600
ACCESS POINT Y SWITCHES	
4	Un (1) paquete - 4 Pack SonicWALL SonicPoint-Ne Dual-Band w/o PoE Injector Internacional
5	SonicWALL PoE Injector 802.3AF Gigabit N
6	Dos (2) switches 24-Port managed PoE stackable Fast Ethernet switch with two combo SFP slots
SERVICIOS PROFESIONALES	
7	Servicios de Instalación y configuración de SOLUCION DEL SONICWALL NSA 3600
8	Servicios de Instalación y configuración de SOLUCION AT-8000GS

Fuente: TRANSMILENIO S.A

A finales del 2014 la Entidad busca diseñar e implementar el esquema de acciones adecuadas para llevar a cabo un test de intrusión ética (Ethical Hacking) e Ingeniería

Social, que permita valorar el estado actual de seguridad de la red y el nivel de concientización de los funcionarios respecto al manejo de seguridad de la información, y que plasme en un informe detallado, los posibles planes de acción y recomendaciones en materia de seguridad, que le posibiliten a TRANSMILENIO S.A., implementar los controles adecuados para eliminar las vulnerabilidades encontradas.

Dentro de las obligaciones de la empresa contratada se encuentran las siguientes:

Realizar Ethical Hacking a direcciones IP internas, externas y aplicaciones informáticas que la entidad indicará.

Desarrollar pruebas de ingeniería social a funcionarios de la entidad para establecer el grado de apropiación y generación de la cultura de la seguridad informática.

Las pruebas a ejecutar deben permitir validar: Seguridad física, seguridad de los equipos, y prácticas de los usuarios internos con respecto a la disposición y tratamiento de la información.

- Realizar levantamiento del inventario y clasificación de los activos de información de TRANSMILENIO S.A., de la siguiente forma: Servidores, equipos de cómputo, dispositivos activos de comunicaciones y aplicaciones informáticas.
- Ejecutar pruebas de vulnerabilidad utilizando herramientas especializadas de escaneo.
- Realizar el proceso de análisis de las vulnerabilidades detectadas, clasificándolas de acuerdo a su grado de criticidad.
- Llevar a cabo la explotación de vulnerabilidades, previas indicaciones impartidas por la Dirección de TIC´s de TRANSMILENIO S.A, presentando informe detallado posterior a su realización.
- Generar propuestas de solución y tratamiento para las vulnerabilidades encontradas.
- Emitir las recomendaciones de carácter preventivo y/o correctivo tendientes a dar el adecuado tratamiento a las vulnerabilidades identificadas.

- Generar los planes de acción correspondientes a las vulnerabilidades identificadas, alineados con estándares internacionales de gestión de riesgos, seguridad informática y mejores prácticas en tecnología.
- Diseñar y ejecutar un plan de sensibilización con base en los resultados obtenidos en la etapa de ingeniería social, con las siguientes características:

- Charla de sensibilización en seguridad de la información, con una duración mínima de 45 minutos, dirigida a usuarios administrativos, técnicos y directivos de la entidad.

- Se dictará en las instalaciones de la entidad.

- Se deben programar como mínimo dos fechas para la ejecución de charla, con el fin de asegurar participación del mayor número de usuarios de la entidad.

El equipo del proyecto deberá estar conformado como mínimo por un (1) Gerente de Proyecto y un (1) consultor Senior en Seguridad de la Información quien deberá acreditar por lo menos una de las siguientes certificaciones: CEH, OPST, OSCP. (SECOP, 2015)

Actualmente el Contrato está ejecutado y en espera de que salgan a la luz pública los resultados del mismo.

En el año 2014 y a inicios del 2015 la oficina de Control interno realizo auditorías Internas, para más claridad al respecto se incluirá en los anexos los informes de auditoría Interna Integral a los siguientes procesos:

PROCESO/ACTIVIDAD: Gestión Jurídica y Contractual

DUEÑO DEL PROCESO: Subgerencia Jurídica

PROCESO/ ACTIVIDAD: Gestión de TIC's

RESPONSABLE DEL PROCESO: Director de TIC's

4. ANALISIS Y EVALUACIÓN DE RIESGOS

Actualmente y de acuerdo con el organigrama de la Entidad, las funciones de la gestión de informática y telecomunicaciones hacen parte de la Subgerencia General.

Para la realización y cumplimiento de las mismas se cuenta con siete Profesionales Especializados, dos Profesionales Universitarios, dos Técnicos de Soporte y un Auxiliar administrativo. Y tiene planteada como misión lo siguiente:

- Dirigir, gestionar y coordinar la planeación, análisis, adquisición, diseño, desarrollo y mejoramiento de los procesos, proyectos y alternativas relacionadas con los sistemas de información, informática y telecomunicaciones de la Entidad.
- Orientar a la Entidad en la planeación, diseño, desarrollo, adquisición, puesta en marcha, uso y mantenimiento de los sistemas de información y de telecomunicaciones, en los que s e soportan los procesos misionales y de apoyo a la gestión de TRANSMILENIO S.A.
- Brindar el soporte y apoyo tecnológico en el diseño, desarrollo, prueba e implementación de los sistemas informáticos de la operación de recaudo del Sistema TransMilenio, de tal forma que las herramientas de hardware, software y telecomunicaciones en las cuales se soportan las tareas de control ejercida por TRANSMILENIO S.A. estén permanentemente disponibles.
- Brindar el soporte y apoyo tecnológico en el diseño, desarrollo, pruebas e implantación de los Sistemas de Información de Control de la Operación del Sistema TransMilenio de tal forma que las herramientas de hardware, software y telecomunicaciones en las cuales se establece la programación y control de la operación estén permanentemente disponible.
- Brindar el soporte y apoyo tecnológico en el diseño, desarrollo, pruebas e implantación de los sistemas informáticos en los que soportan los procesos administrativos de TRANSMILENIO S.A.
- Brindar atención oportuna y eficaz a los requerimientos de usuarios en el uso y operación de las herramientas ofimáticas y garantizar el correcto

funcionamiento de la infraestructura tecnológica y los servicios informáticos y de comunicaciones en los que se soportan los procesos administrativos y operativos de TRANSMILENIO S.A.

4.1. IDENTIFICACIÓN DE RIESGOS

Al Identificar el riesgo en una organización se debe seleccionar la metodología apropiada. En la actualidad, hay diversas metodologías entre otras Octave, Magerit, ISO 27001, etc., para la realización del análisis de riesgo y se cimientan en tres elementos importantes:

- **Activos:** Todos los elementos que necesita una compañía para desarrollar sus actividades misionales, las cuales serán examinadas en el momento del análisis de riesgos. Los activos pueden ser físicos como equipos, servidores, dispositivos de red, etc., y lógicos como bases de datos, software de aplicación, sitios web entre otros.
- **Amenazas:** Todos los eventos que pueden suceder en una organización que afecten directamente los activos en su funcionamiento o en la perdida de la información.
- **Vulnerabilidades:** Todas las debilidades de seguridad que pueden afectar los activos, identificadas en el análisis y que pueden ser explotadas por la amenazas con consecuencias nefastas para la organización.

4.2. INVENTARIO DE HARDWARE, SOFTWARE, APLICACIONES Y SISTEMAS DE INFORMACIÓN.

4.2.1.1. HARDWARE

La compañía cuenta actualmente con equipos de cómputo en la sede Administrativa.

Tabla 2 Inventario Equipos TRANSMILENIO S.A

TIPO	SEDE ADMINISTRATIVA

Computadores de escritorio	300
Computadores portátiles	40
Servidores	20

Fuente: Autoría propia.

Gráfica 8 Detalle estaciones de trabajo TRANSMILENIO S.A

Estaciones de trabajo	ARGOM	CORE I3 DD 500 GB - 1TERA 6 GB RAM
	ASUS	CORE I5 DD 500 GB - 1TERA 4-8 GB RAM
	AVANTE	CORE I3 - CORE I5 DD 500 GB - 1 TERA 6-8 GB RAM
	DELL	CORE 2 DUO - CORE 2 QUAD DD 160 - 500 GB 2-4 GB- RAM
	HP	CORE 2 DUO - CORE I5 DD 80-500 GB 4-6 GB RAM
	JANUS	CORE I3 - CORE I5 - CORE I7 DD 500 GB -1,5 TERAS RAM 4-8 GB
	LENOVO	CORE I3 - CORE I5 DD 160 GB - 500 GB - RAM 2-8 GB
	PCSMART	CORE I3

Fuente: Autoría propia

Gráfica 9 Detalle Servidores TRANSMILENIO S.A.

Servidores	Server-Bd	IBM HS22 (Type 7870) INTEL XEON (BASES DE DATOS)
	Server-Backup	IBM HS22 (Type 7870) INTEL XEON (BCK BASES DE DATOS)
	Server-File	IBM HS22 (Type 7870) INTEL Xeonprocessor MP(ARCHIVO TODOS USUARIOS - SEUS)
	Server-Clouster-1	IBM HS22 (Type 7870) INTEL Xeonprocessor MP(DNS, DHCP, ADFS CORREO EXCHANGE)
	Server-Clouster-2	IBM HS22 (Type 7870) INTEL Xeon MP(DNS, DHCP, ADFS CORREO EXCHANGE)
	Server-IIS64	IBM HS22 (Type 7870) INTEL Xeonprocessor MP(XIPE, SIGET(turnos), SLDF)
	DCMAIN	HP 2 -Way X86 Blade INTEL Xeonprocessor MP (CONTROLADOR PRINCIPAL DE DOMINIO)
	Server-IIS32	IBM HS22 (Type 7870) INTEL Xeonprocessor MP(ROYAL, KACTUS, PIGA)
	Server- SEG	HP PROLIANT XEON (Arch. Temporales -Adm. Kaspersky)
	Server- Alim2	IBM XEON (Archivos Posicionamiento Alimentadores)
	ADFS_1	IBM HS23 (Type 7875) INTEL XEON (Autenticación Correo)
	ADFS_2	IBM HS23 (Type 7875) INTEL XEON (Autenticación Correo)
	TRANSMILENIO	IBM HS23 (Type 7875) INTEL XEON (FILE SERVER)
	MailServer	HP PROLIANT XEON (CONTROLADOR DE DOMINIO ANTERIOR)
	Server - Test	HP PROLIANT XEON (AMBIENTE DE DESARROLLO)
	PISBA	IBM XEON (Soporta BD con la información de los recorridos SAE)

Fuente: TRANSMILENIO S.A 2014.

Esta infraestructura es la que permite las actividades diarias tanto de los funcionarios de la entidad como de las diferentes aplicaciones y servicios con los que se cuenta.

TRANSMILENIO S.A cuenta hoy en día con herramientas ofimáticas, aplicaciones adquiridas en el mercado y desarrollos hechos a la medida según los requerimientos propios del negocio. Por lo tanto **TRANSMILENIO S.A.** cuenta hoy con lo siguiente:

4.2.1.2. APLICATIVOS Y SISTEMAS TMSA

Gráfica 10 Aplicativos y Sistemas TMSA.

NOMBRE APLICATIVO	FUNCIÓN
Sistema de Liquidación y Distribución de Fondos – SLDF	Aplicación que permite hacer liquidación de la tarifa, liquidación a los agentes del sistema y liquidar multas.
Sistema de Control y Regulación de la Operación – SAE	Este sistema transaccional tiene como componentes principales, la programación de la operación diaria y posteriormente la regulación correspondiente. Este sistema es el que registra los sucesos que a diario acontecen en la operación del Sistema TransMilenio y es el que registra todos los eventos de comunicación con la flota de buses troncales
Sistema de Recaudo para Fase I y Fase II:	En el sistema de recaudo se registran a diario las transacciones tanto de ventas como de ingreso y salida de pasajeros dentro del Sistema TransMilenio. Esta aplicación es administrada por los operadores de Recaudo del Sistema de Transporte
Sistema Administrativo y Financiero SEUS SP6	Aplicación del ERP de TRANSMILENIO S.A., maneja los módulos de contabilidad, inventarios, presupuesto, nomina. Activos fijos, contratación, pagos y tesorería.
CORDIS	Aplicativo que maneja el flujo de la correspondencia de la entidad.
SGD (Sistema de Gestión Documental)	Aplicativo que maneja de manera digital las series documentales de la Entidad. Está integrada con el sistema de correspondencia.
Sistema de Recursos Humanos HR – KACTUS	Aplicativo que maneja los módulos de Evaluación de Desempeño, Bienestar y Desarrollo, Selección de personal.
Vehículos y Accidentalidad	Aplicación que maneja la flota de vehículos de Fase I, y II, así como la gestión de los conductores asociados a esa flota.
PIGA (Plan integral de Gestión Ambiental)	Aplicación que maneja la información del Plan Integral de gestión Ambiental.
XIPE (Gestión de Compromisos)	Sistema de información de compromisos de la entidad, en el que se maneja el plan de Acción de TRANSMILENIO S.A.
SIG (Sistema de Información Gerencial)	Bodega de datos que permite mostrar los indicadores de cada uno de los sistemas de gestión de la entidad.
GOALBUS	Sistema que permite generar la programación de la flota.
SCTPSVR	Aplicación que maneja los paneles informativos del sistema.
SIGET	Aplicación que maneja los turnos del personal de la vía y los técnicos de control.
SIG-ALIM	Sistema de Información Geo referencial de Flota alimentadora
ARANDA	Mesa de ayuda para requerimientos de IT
Correo Electrónico	Gestionar servicio de correo.
Sistema de BackUp	Tivoli Storage Manager, Permite hacer tomas automáticas de copia de seguridad de la información de los usuarios.
SQS	Sistema Distrital de quejas y soluciones.
Contratación a la Vista	Portal en el que se realiza la publicación de los procesos de contratación de las entidades del Distrito Capital.
SIPROJ	Permite crear, organizar y buscar información sobre los procesos y demandas que cursan contra entidades del Distrito Capital.

Fuente: TRANSMILENIO S.A.

4.3. RED DE COMUNICACIONES TMSA

Gráfica 11 Red de comunicaciones TRANSMILENIO S.A

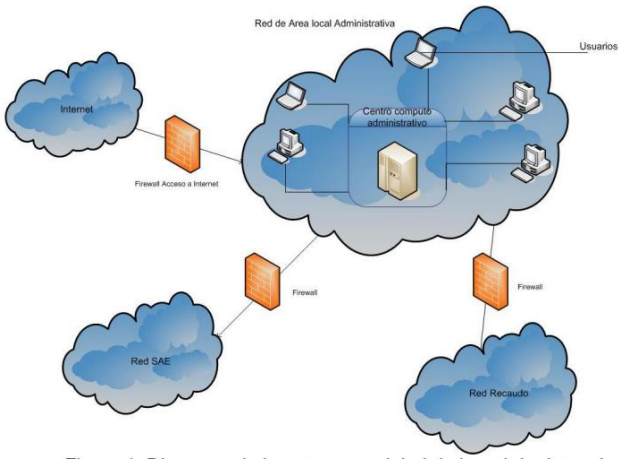
URL Sitio Web	No. de Web masters	Plataforma técnica
www.transmilenio.gov.co www.transportemasivo.com.co www.SITP.gov.co www. Tullave.com	1	▪ Hardware en producción: Procesador: Intel Core 2 Duo 2.13GHz, RAM: 2 GB, Disco duro: 2x120 GB ▪ Sistema operacional: Microsoft Windows 2008 Web Edition; IIS 7 ▪ Bases de datos: Microsoft SQL Server 2005 Standard Edition ▪ Software de desarrollo: Visual Studio 2008 SP1 Professional ▪ Navegador: Internet Explorer 8, Firefox, Chrome

Fuente: TRANSMILENIO S.A.

4.4. ESTRUCTURA GLOBAL RED DE DATOS TRANSMILENIO S.A

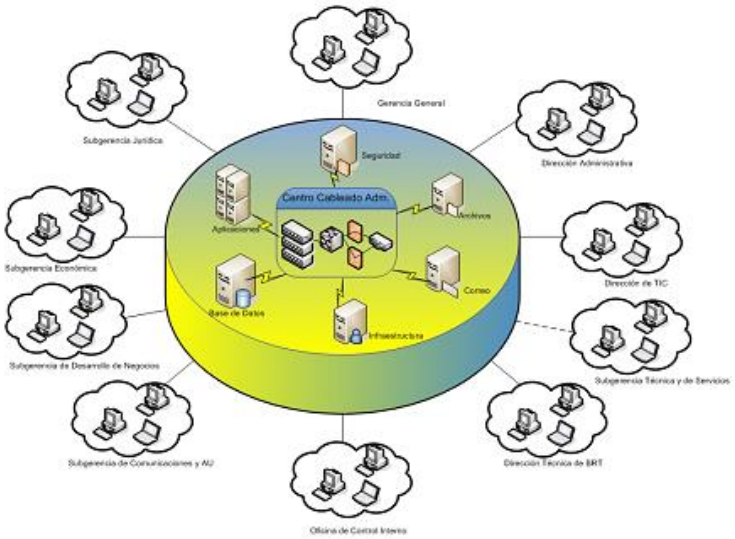
Red corporativa compuesta por tres redes independientes, comunicadas y protegidas por medio de firewalls: SAE (Control de la operación del sistema), Recaudo y Administrativa (interna).

Gráfica 12 Estructura global red de datos TRANSMILENIO S.A.



Fuente: TRANSMILENIO S.A 2014.

Gráfica 13 Diagrama configuración red administrativa TRANSMILENIO S.A.



Fuente: TRANSMILENIO S.A.

4.5. INFRAESTRUCTURA DE SEGURIDAD TRANSMILENIO S.A.

Gráfica 14 Infraestructura de seguridad TRANSMILENIO S.A

No.	CONCEPTO
1	Antivirus Kaspersky – Anti Spam
2	Firewall Recaudo
3	Firewall Centro de Control
4	Firewall entre Centro de Control y Recaudo
5	Firewall de Acceso a Internet, Filtro de Contenido
6	Filtro de Contenido
7	Políticas de Controlador de dominio
8	Políticas de Seguridad Informática

Fuente: TRANSMILENIO S.A.

4.6. IDENTIFICACIÓN DE ACTIVOS

Tabla 3: Identificación de activos

Tipo de activo	Nombre
Datos	Datos de usuario (Información confidencial), documentos, Contratos, normas, resoluciones, etc.
Software	Sistemas de información
	Software de ofimática
	Bases de datos
	Navegador web
	Software de diseño
	Sistemas operativos PC/Servidor
	Correo electrónico
Físicos	Servidores
	Estaciones de trabajo
	Firewalls
	Dispositivos de conectividad (AP, módem, router, switch)
	Cuarto de comunicaciones
	Cableado Estructurado
	Medios de almacenamiento(CD, DVD, USB)
	Dispositivos móviles
	Impresoras
Equipamiento auxiliar	UPS, sistemas de detección, sistemas de enfriamiento, Cableado estructurado, instalaciones eléctricas

Fuente: Autoría propia

4.7. IDENTIFICACIÓN DE SERVICIOS

Tabla 4: identificación de servicios

Servicios de red	Autenticación
	DNS
	DHCP
	Impresión
	Comunicaciones
	Email
	Internet
	Cloud computing
	Intranet
	Bases de datos
	Wifi

Fuente: Autoría propia

AMENAZAS DE SEGURIDAD

Tabla 5: Amenazas de seguridad

Vulnerabilidad	Amenaza	Ataque
Gestión de contraseñas inadecuada	Divulgación de Contraseñas, Manipulación no autorizada	Ingeniería social, hacking
Falta de equipos de sensibilidad a los cambios en el voltaje	Fallas técnicas por sobre-voltajes en la infraestructura tecnológica	Tormentas eléctrica, Manos criminales
Seguridad del cableado inadecuada	Acceso no autorizado, fallas, cortes de corriente	Manos criminales
Mantenimiento inadecuado	Funcionamiento inadecuado de los equipos	Virus
Copias de seguridad inadecuadas o irregulares	Perdida de Información	Hacking

Protección inadecuada de claves criptográficas	Divulgación de Contraseñas, Manipulación no autorizada	Hacking
Falta de procedimiento a la terminación del empleo para la eliminación de los derechos de acceso.	Perdida de Información, Acceso no autorizado	Hacking
La falta de protección para equipos móviles	Perdida de Información, Acceso no autorizado	Hacking
La falta de sistemas de identificación y autenticación	Intrusiones, Perdida de Información, Acceso no autorizado	Hacking, spoofing, análisis de tráfico, MitM, Acceso remoto, Jamming
Vulnerabilidad de denegación del servicio	Caída de servicios, perdida de conexión	Ataque de denegación de servicios
Deficiencias organizacionales	Intrusiones, Perdida de Información, Acceso no autorizado	Manos criminales, Hacking
Personal no calificado	Errores de procesamiento, servicios no solicitados, Acceso no autorizado	Manos criminales, Hacking
Descarga sin control de Internet	Funcionamiento inadecuado de los equipos y la red de datos	Virus

Fuente: Autoría propia.

Después de obtener la lista de vulnerabilidades y amenazas, se hace una lista de los posibles riesgos informáticos, y se agrupan por categorías (hardware, software, redes, comunicaciones, seguridad física, seguridad lógica, personal del área, entre otros). Una vez se listan los riesgos, se realiza un cuadro de evaluación de riesgos por probabilidad e impacto, usando una escala cualitativa, por ejemplo: la escala para probabilidad puede tener los valores (bajo, medio, alto), y para impacto los valores de (leve, moderado, catastrófico), esta valoración se hace de acuerdo a la probabilidad de ocurrencia de riesgos (número de veces por periodo de tiempo) y el impacto (las consecuencias de llegar a concretarse el riesgo). Finalmente se llevan los riesgos identificados a una matriz de riesgos donde se puede apreciar cuales son los de mayor impacto y mayor probabilidad.

4.8. PLANEACIÓN DEL ANÁLISIS DE RIESGOS

Hoy es imposible hablar de un sistema cien por cien seguro, sin incurrir en altos costos, aun así no estaremos totalmente seguros de ahí que es necesario asumir riesgos, la solución a medias, entonces, sería acotar todo el espectro de seguridad, en lo que hace a plataformas, procedimientos y estrategias, de esta manera se puede controlar todo un conjunto de vulnerabilidades, aunque no se logre la seguridad total.

Algunas organizaciones desarrollan documentos, directrices y recomendaciones que orientan en el uso adecuado de las nuevas tecnologías para obtener el mayor provecho y evitar el uso indebido de la mismas, en este sentido, las Políticas de Seguridad Informática, surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos.

La evaluación de riesgos y presentación de respuestas debe prepararse de forma personalizada para cada organización.

4.9. RIESGOS

Tabla 6: Riesgos TMSA

RIESGOS
Usuarios sin restricciones
Claves evidentes y compartidas
Relación de confianza entre equipos
Manuales de software y de procedimientos desactualizados o inexistentes
Actualizaciones de seguridad (Parches)
Falta de dispositivos de detección de intrusos
Falta de herramientas de análisis de tráfico en la red
Alta disponibilidad
Comunicaciones
Cloud computing
Falta de políticas sobre Backups
No hay la suficiente capacitación sobre seguridad informática
Seguridad física
Hacking

Fuente: Autoría propia.

4.9.1.1. RIESGO INHERENTE

Es el riesgo que un servicio plantea si no hay controles u otros factores atenuantes, en otras palabras es el riesgo antes de aplicar controles.

Gráfica 15 Valoración del riesgo

VALORACION DEL RIESGO	
NIVEL DE RIESGO INHERENTE	CALIFICACION
EXTREMO	41 A 60
ALTO	21 A 40
MODERADO	11 A 20
BAJO	1 A 10

Fuente: Autoría propia.

MEDICIÓN RIESGO INHERENTE

Gráfica 16 Tabla medición riesgo

PROBABILIDAD	VALOR			
ALTA	3	15 Zona de riesgo moderado evitar el riesgo	30 Zona de riesgo importante Reducir el riesgo Evitar el riesgo Compartir o transferir	60 Zona de riesgo inaceptable Reducir el riesgo Evitar el riesgo Compartir o transferir
MEDIA	2	10 Zona de riesgo tolerable Asumir el riesgo Reducir el riesgo	20 Zona de riesgo moderado Reducir el riesgo Evitar el riesgo Compartir o transferir	40 Zona de riesgo importante Reducir el riesgo Evitar el riesgo Compartir o transferir
BAJA	1	5 Zona de riesgo aceptable Asumir el riesgo	10 Zona de riesgo tolerable Reducir el riesgo Compartir o transferir	20 Zona de riesgo moderado Reducir el riesgo Compartir o transferir
	IMPACTO	Leve	Moderado	Catastrófica
	VALOR	5	10	20

Fuente: Autoría propia.

Gráfica 17 análisis de riesgos Datos de usuario

			Medición - Riesgo Inherente			
Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	TOTAL NIVEL DE EXPOSICIÓN	ZONA DE RIESGO	ESTRATEGIA DE ADMINISTRACIÓN DE RIESGOS SUGERIDA	Vulnerabilidad
Datos de usuario	(Información confidencial).	Documentos, Contratos, normas, resoluciones, etc.	40	ZONA DE RIESGO IMPORTANTE	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	ALTA

Fuente: Autoría propia.

En el análisis de riesgo de los datos de usuario se evidencia una zona de riesgo importante y una vulnerabilidad alta antes de aplicar controles.

Gráfica 18 análisis de riesgos Sistemas de información

			Medición - Riesgo Inherente			
Sistemas de información	SIG (Sistema de Información Gerencial)	Bodega de datos que permite mostrar los indicadores de cada uno de los sistemas de gestión de la entidad.	5	ZONA DE RIESGO ACEPTABLE	ASUMIR EL RIESGO	BAJA
	GOALBUS	Sistema que permite generar la programación de la flota.	40	ZONA DE RIESGO IMPORTANTE	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	ALTA
	SIG-ALIM	Sistema de Información Geo referencial de Flota alimentadora	40	ZONA DE RIESGO IMPORTANTE	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	ALTA
	ARANDA	Mesa de ayuda para requerimientos de IT	5	ZONA DE RIESGO ACEPTABLE	ASUMIR EL RIESGO	BAJA
	Sistema de BackUp Tivoli Storage Manager	Permite hacer tomas automáticas de copia de seguridadde la información de los usuarios.	40	ZONA DE RIESGO IMPORTANTE	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	ALTA
	Contratación a la Vista	Portal en el que se realiza la publicación de los procesos de contratación de las entidades del Distrito Capital.	20	ZONA DE RIESGO MODERADO	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	MEDIA
	SECOP	Portal en el que se realiza la publicación de los procesos de contratación a nivel	20	ZONA DE RIESGO MODERADO	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	MEDIA
	SIPROJ	Permite crear, organizar y buscar información sobre los procesos y demandas que cursan contra entidades del Distrito Capital.	20	ZONA DE RIESGO MODERADO	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	MEDIA

Fuente: Autoría propia.

En el análisis de riesgo de los sistemas de información se evidencia una zona de riesgo importante y una vulnerabilidad alta antes de aplicar controles en aplicaciones como GOALBUS, SIG-ALIM Y el sistema de BackUp Tivoli Storage Manager.

Gráfica 19 análisis de riesgos Software de ofimática

			Medición - Riesgo Inherente			
Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	TOTAL NIVEL DE EXPOSICIÓN	ZONA DE RIESGO	ESTRATEGIA DE ADMINISTRACIÓN DE RIESGOS SUGERIDA	Vulnerabilidad
Software de ofimática	Office 2010		10	ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL RIESGO	BAJA
	Office 2007		10	ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL RIESGO	BAJA
	ADOBE ACROBAT		10	ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL RIESGO	BAJA
	ADOBE PHOTOSHOP		10	ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL RIESGO	BAJA
	MICROSOFT VISIO PROFESSIONAL		10	ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL RIESGO	BAJA
	MICROSOFT ACCESS		10	ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL RIESGO	BAJA
	MICROSOFT PROJECT		10	ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL RIESGO	BAJA

Fuente: Autoría propia.

En el análisis de riesgo al software de ofimática se evidencia una zona de riesgo tolerable y una vulnerabilidad baja antes de aplicar controles en estas aplicaciones.

Gráfica 20 análisis de riesgo a las Bases de datos y al Correo electrónico.

			Medición - Riesgo Inherente			
Servicio	**Nombre Servidor / Máquina Virtual / Activo**	**Descripción**	**TOTAL NIVEL DE EXPOSICIÓN**	**ZONA DE RIESGO**	**ESTRATEGIA DE ADMINISTRACIÓN DE RIESGOS SUGERIDA**	**Vulnerabilidad**
Bases de datos	Microsoft SQL Server 2005 Standard Edition		**40**	**ZONA DE RIESGO IMPORTANTE**	**REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR**	**ALTA**
	ORACLE		**40**	**ZONA DE RIESGO IMPORTANTE**	**REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR**	**ALTA**
Navegador web	Internet Explorer, Firefox, Chrome		**10**	ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL RIESGO	**BAJA**
Correo electrónico	CORREO EXCHANGE	Gestionar servicio de correo.	**40**	**ZONA DE RIESGO IMPORTANTE**	**REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR**	**ALTA**

Fuente: Autoría propia.

En el análisis de riesgo a las Bases de datos y al Correo electrónico se evidencia una zona de riesgo importante y una vulnerabilidad alta antes de aplicar controles en estas aplicaciones.

Gráfica 21 análisis de riesgo a las Sistemas operativos.

			Medición - Riesgo Inherente			
Servicio	**Nombre Servidor / Máquina Virtual / Activo**	**Descripción**	**TOTAL NIVEL DE EXPOSICIÓN**	**ZONA DE RIESGO**	**ESTRATEGIA DE ADMINISTRACIÓN DE RIESGOS SUGERIDA**	**Vulnerabilidad**

			Medición - Riesgo Inherente			
Software de diseño	AUTOCAD		10	ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL RIESGO	BAJA
	COREL DRAW		10	ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL RIESGO	BAJA
	ADOBE PHOTOSHOP		10	ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL RIESGO	BAJA
Sistemas operativos PC/Servidor	WINDOWS 7 PRO		20	ZONA DE RIESGO MODERADO	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	MEDIA
	WINDOWS XP PRO		20	ZONA DE RIESGO MODERADO	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O	MEDIA
	Windows XP		20	ZONA DE RIESGO MODERADO	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O	MEDIA
	LINUX Red Hat		40	ZONA DE RIESGO IMPORTANTE	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	ALTA
	Windows Server 2000		40	ZONA DE RIESGO IMPORTANTE	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	ALTA
	Windows Sever 2008 R2 SP 2		40	ZONA DE RIESGO IMPORTANTE	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	ALTA

Fuente: Autoría propia.

En el análisis de riesgo a las Sistemas operativos se evidencia una zona de riesgo importante y una vulnerabilidad alta antes de aplicar controles en los sistemas operativos de servidor.

Gráfica 22 análisis de riesgo a los aplicativos a la medida

			Medición - Riesgo Inherente			
Aplicativos a la medida	Sistema Administrativo y Financiero SEUS SP6 .	Aplicación del ERP de TRANSMILENIO S.A. Maneja los módulos de contabilidad,inventarios, presupuesto, nomina. Activos fijos,contratación, pagos y tesorería.	**40**	**ZONA DE RIESGO IMPORTANTE**	**REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR**	**ALTA**
	CORDIS	Aplicativo que maneja el flujo de la correspondencia de la entidad.	**40**	**ZONA DE RIESGO IMPORTANTE**	**REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR**	**ALTA**
	SGD (Sistema de Gestión Documental)	Aplicativo que maneja de manera digital las series documentales de la Entidad. Está integrada con el sistema de correspondencia.	**20**	ZONA DE RIESGO MODERADO	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	**MEDIA**
	Sistema de Recursos Humanos HR – KACTUS	Aplicativo que maneja los módulos de Evaluación de Desempeño, Bienestar y Desarrollo, Selección de personal.	**5**	ZONA DE RIESGO ACEPTABLE	ASUMIR EL RIESGO	**BAJA**
	Vehículos y Accidentalidad	Aplicación que maneja la flota de vehículos de Fase I, y II, así como la gestión de los conductores asociados a esa flota.	**20**	ZONA DE RIESGO MODERADO	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	**MEDIA**
	PIGA (Plan integral de Gestión Ambiental)	Aplicación que maneja la información del Plan Integral de gestión Ambiental.	**5**	ZONA DE RIESGO ACEPTABLE	ASUMIR EL RIESGO	**BAJA**
	Sistema de Liquidación y Distribución de Fondos – SLDF	Aplicación que permite hacer liquidación de la tarifa, liquidación a los agentes del sistema y liquidar multas.	**20**	ZONA DE RIESGO MODERADO	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	**MEDIA**
	SCTPSVR	Aplicación que maneja los paneles informativos del sistema.	**20**	ZONA DE RIESGO MODERADO	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	**MEDIA**
	SIGET	Aplicación que maneja los turnos del personal de la vía y los técnicos de control.	**20**	ZONA DE RIESGO MODERADO	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	**MEDIA**
Antivirus	Antivirus Kaspersky – Anti Spam	Aplicación Antivirus	**20**	ZONA DE RIESGO MODERADO	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	**MEDIA**

Fuente: Autoría propia.

En el análisis de riesgo a los aplicativos a la medida (SEUS, CORDIS, SGD, etc.) se evidencia una zona de riesgo importante y una vulnerabilidad alta antes de aplicar controles en aplicaciones como SEUS y CORDIS.

Gráfica 23 análisis de riesgo a los Servidores.

			Medición - Riesgo Inherente			
Servidores	Server-IIS64	IBM HS22 (Type 7870) INTEL Xeonprocessor MP(XIPE, SIGET(turnos), SLDF)	**40**	**ZONA DE RIESGO IMPORTANTE**	**REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR**	**ALTA**
	DCMAIN	HP 2 -Way X86 Blade INTEL Xeonprocessor MP (CONTROLADOR PRINCIPAL DE DOMINIO)				
	Server-IIS32	IBM HS22 (Type 7870) INTEL Xeonprocessor MP(ROYAL, KACTUS, PIGA)				
		COMPAQ INTEL X86 (MANEJO INGRESOC.CONTROL)				
	Server- SEG	HP PROLIANT XEON (Arch. Temporales -Adm. Kaspersky)				
	Server- Alim2	IBM XEON (Archivos Posicionamiento Alimentadores)				
	ADFS_1	IBM HS23 (Type 7875) INTEL XEON (Autenticación Correo)				
	ADFS_2	IBM HS23 (Type 7875) INTEL XEON (Autenticación Correo)				
	TRANSMILENIO	IBM HS23 (Type 7875) INTEL XEON (FILE SERVER)				
	MailServer	HP PROLIANT XEON (CONTROLADOR DE DOMINIO ANTERIOR)				
	Server - Test	HP PROLIANT XEON (AMBIENTE DE DESARROLLO)				
	PISBA	IBM XEON (Soporta BD con la información de los recorridos SAE)				
	COLON	HP PROLIANT X86 (BCK DE PISBA - SAE)				

Fuente: Autoría propia.

En el análisis de riesgo a los Servidores se evidencia una zona de riesgo importante y una vulnerabilidad alta antes de aplicar controles.

Gráfica 24 análisis de riesgo a las estaciones de trabajo.

			Medición - Riesgo Inherente			
Servicio	**Nombre Servidor / Máquina Virtual / Activo**	**Descripción**	**TOTAL NIVEL DE EXPOSICIÓN**	**ZONA DE RIESGO**	**ESTRATEGIA DE ADMINISTRACIÓN DE RIESGOS SUGERIDA**	**Vulnerabilidad**
Estaciones de trabajo	ARGOM	CORE I3 DD 500 GB - 1 TERA 6 GB RAM	**30**	ZONA DE RIESGO IMPORTANTE	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	ALTA
	ASUS	CORE I5 DD 500 GB - 1 TERA 4-8 GB RAM				
	AVANTE	CORE I3 - CORE I5 DD 500 GB - 1 TERA 6-8 GB RAM				
	DELL	CORE 2 DUO - CORE 2 QUAD DD 160 - 500 GB 2-4 GB- RAM				
	HP	CORE 2 DUO - CORE I5 DD 80-500 GB 4-6 GB RAM				
	JANUS	CORE I3 - CORE I5 - CORE I7 DD 500 GB -1,5 TERAS RAM 4-8 GB				
	LENOVO	CORE I3 - CORE I5 DD 160 GB - 500 GB - RAM 2-8 GB				
	PCSMART	CORE I3				
Firewalls	DELL SonicWall NSA 3500	Seguridad Perimetral	**20**	ZONA DE RIESGO MODERADO	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	MEDIA
	Dell SonicWALL Network Security Appliance NSA 3600					
	Dell SonicWALLHigh Availability (HA) Unit NSA 3600					

Fuente: Autoría propia.

En el análisis de riesgo a las estaciones de trabajo se evidencia una zona de riesgo importante y una vulnerabilidad alta antes de aplicar controles.

Gráfica 25 análisis de riesgo al Cuarto de comunicaciones y a las comunicaciones.

			Medición - Riesgo Inherente			
Servicio	**Nombre Servidor / Máquina Virtual / Activo**	**Descripción**	**TOTAL NIVEL DE EXPOSICIÓN**	**ZONA DE RIESGO**	**ESTRATEGIA DE ADMINISTRACIÓN DE RIESGOS SUGERIDA**	**Vulnerabilidad**
Cuarto de comunicaciones		RACKS, CABLEADO, DISPOSITIVOS DE RED	40	ZONA DE RIESGO IMPORTANTE	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	ALTA
Cableado Estructurado		CAT 6	10	ZONA DE RIESGO ACEPTABLE	ASUMIR EL RIESGO	BAJA
Medios de almacenamiento	CD-DVD USB CAMARAS		10	ZONA DE RIESGO ACEPTABLE	ASUMIR EL RIESGO	BAJA
Dispositivos móviles	CELULARES TABLETS		5	ZONA DE RIESGO ACEPTABLE	ASUMIR EL RIESGO	BAJA
Impresoras			20	ZONA DE RIESGO MODERADO	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	MEDIA
UPS, sistemas de detección, sistemas de enfriamiento, instalaciones eléctricas			20	ZONA DE RIESGO MODERADO	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	MEDIA
Comunicaciones			40	ZONA DE RIESGO IMPORTANTE	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	ALTA

Fuente: Autoría propia.

En el análisis de riesgo al Cuarto de comunicaciones y a las comunicaciones (Telefonía y Transmisión de datos) se evidencia una zona de riesgo importante y una vulnerabilidad alta antes de aplicar controles.

Gráfica 26 análisis de riesgo al servicio de Internet, Cloud computing, Intranet y Wifi

			Medición - Riesgo Inherente				
Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	TOTAL NIVEL DE EXPOSICIÓN	ZONA DE RIESGO	ESTRATEGIA DE ADMINISTRACIÓN DE RIESGOS SUGERIDA	Vulnerabilidad	
Internet			20	ZONA DE RIESGO MODERADO	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	MEDIA	
Cloud computing			20	ZONA DE RIESGO MODERADO	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	MEDIA	
Intranet			20	ZONA DE RIESGO MODERADO	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	MEDIA	
Vifi			20	ZONA DE RIESGO MODERADO	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	MEDIA	

Fuente: Autoría propia.

Finalmente al realizar el análisis de riesgo al servicio de Internet, Cloud computing, Intranet y Wifi se evidencia una zona de riesgo moderado y una vulnerabilidad media antes de aplicar controles.

Resultados:

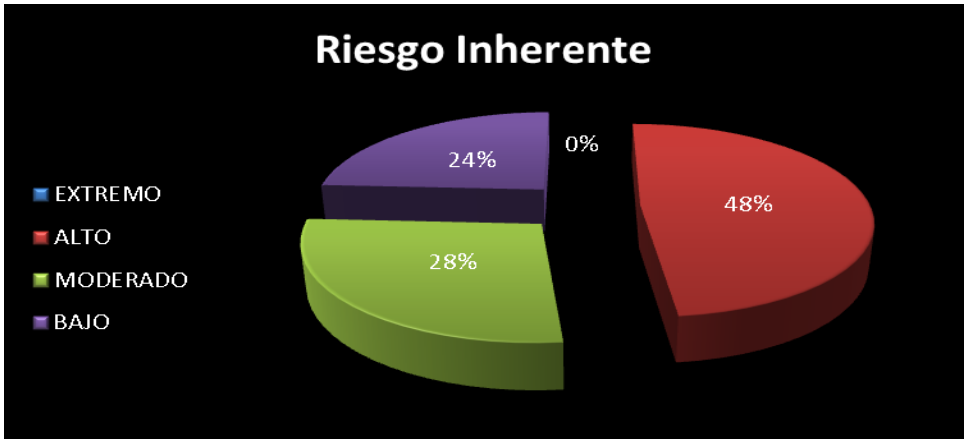
Riesgo Inherente

Tabla 7 Calculo Riesgo Inherente

Riesgo Inherente	Total
EXTREMO	0
ALTO	44
MODERADO	25
BAJO	22
TOTALES	**91**

Fuente: Autoría propia.

Gráfica 27 Riesgo Inherente



Fuente: Autoría propia.

4.9.1.2. RIESGO RESIDUAL

El nivel de riesgo residual, es el riesgo que la organización consigue asumir después de aplicar medidas o salvaguardias de seguridad tratadas en la matriz de riesgo. El riesgo residual es la pérdida que existe aun cuando se han implementado salvaguardas que han sido implantadas para proteger a los recursos de información de sus amenazas.

El proceso de análisis genera la matriz de riesgo, en esta se ilustran los elementos identificados, sus relaciones y los cálculos realizados, la suma de los riesgos residuales calculados es la exposición neta total de la compañía a los riesgos.

Gráfica 7 Valoración del riesgo

VALORACION DEL RIESGO (residual)	
NIVEL DE RIESGO	CALIFICACION
EXTREMO	> 37
ALTO	23 a 36
MODERADO	9 a 22
BAJO	<8

Fuente: Autoría propia.

Descripción matriz de riesgos

- Cada fila representa una amenaza
- La columna probabilidad indica cuán probable es que actué la amenaza, independiente de los controles establecidos. La certeza es el 100% y la imposibilidad es 0%. Los porcentajes en cada fila son trabajados de manera independiente.
- Las siguientes columnas evidencian para cada uno de los activos a proteger el valor de la perdida media estimada que causaría la amenaza en el activo.
- Los anteriores datos permiten calcular la siguiente columna, el riesgo total el cual suma los productos de la probabilidad de la amenaza por el impacto, de toda la fila.

- Consecutivamente se señala la efectividad del control, lo cual indica que el riesgo total se puede mitigar. Un ejemplo seria la implementación de seguridad perimetral (Firewall, IDS, Proxy, IDS, IDPS, etc.) mitigaría accesos no autorizados vía internet.
- Finalmente, en la última columna, se demuestra cual es el riesgo residual, que resulta al aplicar la efectividad del control al riesgo total.

Gráfica 29 análisis de riesgo de los datos de usuario

						Medición - Riesgo Residual		
Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Control para Frecuencia	Control para Impacto	ZONA DE RIESGO	ESTRATEGIA DE ADMINISTRACIÓN DE RIESGOS SUGERIDA	Vulnerabilidad
Datos de usuario	(Información confidencial),	Documentos, Contratos, normas, resoluciones, etc.	Abuso de derechos (de usuario, administrador) Acceso no autorizado (a oficinas, edificio, sala, centro de computo, sistema de información, documentación, información, entre otros).	Seguridad Perimetral, Políticas de claves seguras, Copias de seguridad,	PLAN DE CONTINUIDAD DEL NEGOCIO	ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL RIESGO	BAJA

Fuente: Autoría propia.

En el análisis de riesgo de los datos de usuario se evidencia una zona de riesgo tolerable y una vulnerabilidad baja después de aplicar controles.

Gráfica 30 análisis de riesgo de los sistemas de información.

	Nombre					Medición - Riesgo Residual		
Servicio	**Servidor / Máquina Virtual / Activo**	**Descripción**	**Evento de Riesgo**	**Control para Frecuencia**	**Control para Impacto**	**ZONA DE RIESGO**	**ESTRATEGIA DE ADMINISTRACIÓN DE RIESGOS**	**Vulnerabilidad**
Sistemas de información	Sistema de Control y Regulación de la Operación – SAE	Este sistema transaccional tiene como componentes principales, la programación de la operación diaria y posteriormente la regulación correspondiente. Este sistema es el que registra los sucesos que a diario acontecen en la operación del Sistema TransMilenio y es el que registra todos los eventos de comunicación con la flota de buses troncales	Saturación del sistema de información Errores de transmision o almacenamiento Avería de origen físico o lógico Errores de mantenimiento / actualización de programas (software) Abuso de privilegios de acceso Suplantación de la identidad del usuario Vulnerabilidades de los programas	Analisis de trafico, calidad en servicios ISP, mantenimiento correctivo y preventivo, revisión de roles de usuarios, politicas de claves seguras, antivirus, copias de seguridad, seguridad perimetral, soporte proveesor	Soporte proveedor	ZONA DE RIESGO MODERADO	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	MEDIA
	Sistema de Recaudo para Fase I y Fase II:	En el sistema de recaudo se registran a diario las transacciones tanto de ventas como de ingreso y salida de pasajeros dentro del Sistema TransMilenio. Esta aplicación es administrada por los operadores de Recaudo del Sistema deTransporte				ZONA DE RIESGO MODERADO	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	MEDIA
	SIG (Sistema de Información Gerencial)	Bodega de datos que permite mostrar los indicadores de cada uno de los sistemas de gestión de la entidad.				ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL RIESGO	BAJA
	GOALBUS	Sistema que permite generar la programación de la flota.				ZONA DE RIESGO MODERADO	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O	MEDIA
	SIG-ALIM	Sistema de Información Geo referencial de Flota alimentadora				ZONA DE RIESGO MODERADO	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O	MEDIA
	ARANDA	Mesa de ayuda para requerimientos de IT				RIESGO TOLERABLE	ASUMIR EL RIESGO,	BAJA
	Sistema de BackUp Tivoli Storage Manager	Permite hacer tomas automáticas de copia de seguridadde la información de los usuarios.				ZONA DE RIESGO MODERADO	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	MEDIA
	Contratación a la Vista	Portal en el que se realiza la publicación de los procesos de contratación de las entidades del Distrito Capital.				ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL RIESGO	BAJA
	SECOP	Portal en el que se realiza la publicación de los procesos de contratación a nivel nacional.				ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL RIESGO	BAJA
	SIPROJ	Permite crear, organizar y buscar información sobre los procesos y demandas que cursan contra entidades del Distrito Capital.				ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL RIESGO	BAJA

Fuente: Autoría propia.

En el análisis de riesgo de los sistemas de información se evidencia una zona de riesgo moderado y una vulnerabilidad media después de aplicar controles en aplicaciones como GOALBUS, SIG-ALIM Y el sistema de BackUp Tivoli Storage Manager.

Gráfica 31 análisis de riesgo a las Bases de datos

B	C	D	E	L	M	Q	R	S
	Nombre					Medición - Riesgo Residual		
Servicio	Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Control para Frecuencia	Control para Impacto	ZONA DE RIESGO	ESTRATEGIA DE ADMINISTRACIÓN DE RIESGOS	Vulnerabilid
Software de ofimática	Micrasoft Office 365		Errores de los usuarios Vulnerabilidades de los programas (software) Errores de mantenimiento / actualización de programas (software) Difusión de software dañina Uso de software no licenciado o no autorizado	Antivirus, mantenimiento correctivo y preventivo, políticas de seguridad	Soporte proveedor	ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL	BAJA
	Office 2010					ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL	BAJA
	Office 2007					ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL RIESGO	BAJA
	ADOBE ACROBAT					ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL	BAJA
	ADOBE PHOTOSHOP					ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL	BAJA
	MICROSOFT VISIO PROFESSIONAL					ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL	BAJA
	MICROSOFT ACCESS					ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL	BAJA
	MICROSOFT PROJECT					ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL	BAJA
Bases de datos	Micrasoft SQL Server 2005 Standard Edition		Errores de los usuarios Saturación del sistema de información Errores de transmisión o almacenamiento Avería de origen física o lógica Errores de mantenimiento / actualización de programas (software) Abuso de privilegios de acceso Suplantación de la identidad del usuario Vulnerabilidades de los programas (software)	Analizar de trafico, calidad en servicios ISP, mantenimiento correctivo y preventivo, revisión de roles de usuarios, políticas de claves seguras, antivirus, copias de seguridad, soporte proveedor	Soporte proveedor	ZONA DE RIESGO MODERADO	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	MEDIA
	ORACLE					ZONA DE RIESGO MODERADO	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	MEDIA

Fuente: Autoría propia.

En el análisis de riesgo a las Bases de datos se evidencia una zona de riesgo moderado y una vulnerabilidad media después de aplicar controles en estas aplicaciones.

Gráfica 32 análisis de riesgo al correo electrónico y los Sistemas operativos de Servidor.

						Medición - Riesgo Residual		
Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Control para Frecuencia	Control para Impacto	ZONA DE RIESGO	ESTRATEGIA DE ADMINISTRACIÓN DE RIESGOS SUGERIDA	Vulnerabilidad
Navegador web	Internet Explorer, Firefox, Chrome		Errores de los usuarios Vulnerabilidades de los programas (software Errores de mantenimiento / actualización de programas (software) Difusión de software dañino	Analisis de trafico, calidad en servicios ISP, mantenimiento correctivo y preventivo, revisión de roles de usuarios, politicas de claves seguras, antivirus	Soporte proveedor	ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL RIESGO	BAJA
Correo electrónico	CORREO EXCHANGE	Gestionar servicio de correo.	Vulnerabilidades de los programas (software) Errores de mantenimiento / actualización de programas (software) Difusión de software dañino Saturación del sistema de información Errores de transmision o almacenamiento Avería de origen físico o lógico	Analisis de trafico, calidad en servicios ISP, mantenimiento correctivo y preventivo, revisión de roles de usuarios, politicas de claves seguras, antivirus	PLAN DE CONTINUIDAD DEL NEGOCIO	ZONA DE RIESGO MODERADO	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	MEDIA

	Nombre					Medición - Riesgo Residual		
Servicio	Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Control para Frecuencia	Control para Impacto	ZONA DE RIESGO	ESTRATEGIA DE ADMINISTRACIÓN DE RIESGOS	Vulnerabilidad
Software de diseño	AUTOCAD		Errores de los usuarios Vulnerabilidades de los programas (software) Errores de mantenimiento / actualización de programas (software) Uso de software no licenciado o no autorizado Avería de origen físico o lógico	Antivirus, mantenimiento correctivo y preventivo, revisión de roles de usuarios,	Soporte proveedor	ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL RIESGO	BAJA
	COREL DRAW					ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL	BAJA
Sistemas operativos PC/Servidor	WINDOWS 7 PRO		Errores de los usuarios Saturación del sistema de información Errores de transmision o almacenamiento Avería de origen físico o lógico Errores de mantenimiento / actualización de programas (software) Abuso de privilegios de acceso Suplantación de la identidad del usuario Vulnerabilidades de los programas (software)	Analisis de trafico, calidad en servicios ISP, mantenimiento correctivo y preventivo, revisión de roles de usuarios, políticas de claves seguras, antivirus, Firewalls, copias de seguridad	PLAN DE CONTINUIDAD DEL NEGOCIO	ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL RIESGO	BAJA
	WINDOWS XP PRO					ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL	BAJA
	Windows XP					ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL	BAJA
	Windows Server 2000					ZONA DE RIESGO MODERADO	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O	MEDIA
	Windows Sever 2008 R2 SP 2					ZONA DE RIESGO MODERADO	REDUCIR EL RIESGO, EVITAR EL RIESGO,	MEDIA

Fuente: Autoría propia.

En el análisis de riesgo al correo electrónico y los Sistemas operativos de Servidor evidencia una zona de riesgo moderado y una vulnerabilidad media después de aplicar controles.

Gráfica 33 análisis de los aplicativos a la medida y al antivirus.

						Medición - Riesgo Residual		
Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Control para Frecuencia	Control para Impacto	ZONA DE RIESGO	ESTRATEGIA DE ADMINISTRACIÓN DE RIESGOS SUGERIDA	Vulnerabilidad
Aplicativos a la medida	Sistema Administrativo y Financiero SEUS SP6	Aplicación del ERP de TRANSMILENIO S.A. Maneja los módulos de contabilidad,inventarios, presupuesto, nomina. Activos fijos,contratación, pagos y tesorería.	Errores de los usuarios Saturación del sistema de información Errores de transmision o almacenamiento Avería de origen físico o lógico Errores de mantenimiento / actualización de programas software) Abuso de privilegios de acceso Suplantación de la identidad del usuario Vulnerabilidades de los programas (software)	Analisis de trafico, calidad en servicios ISP, mantenimiento correctivo y preventivo, revisión de roles de usuarios, politicas de claves seguras, antivirus, Firewalls, copias de seguridad	PLAN DE CONTINUIDAD DEL NEGOCIO	ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL RIESGO	BAJA
	CORDIS	Aplicativo que maneja el flujo de la correspondencia de la entidad.				ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL RIESGO	BAJA
	SGD (Sistema de Gestión Documental)	Aplicativo que maneja de manera digital las series documentales de la Entidad. Está integrada con el sistema de correspondencia.				ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL RIESGO	BAJA
	Sistema de Recursos Humanos HR – KACTUS	Aplicativo que maneja los módulos de Evaluación de Desempeño, Bienestar y Desarrollo, Selección de personal.				ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL RIESGO	BAJA
	Vehículos y Accidentalidad	Aplicación que maneja la flota de vehículos de Fase I, y II, así como la gestión de los conductores asociados a esa flota.				ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL RIESGO	BAJA
	PIGA (Plan integral de Gestión Ambiental)	Aplicación que maneja la información del Plan Integral de gestión Ambiental.				ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL RIESGO	BAJA
	Sistema de Liquidación y Distribución de Fondos –	Aplicación que permite hacer liquidación de la tarifa, liquidación a los agentes del sistema y liquidar multas.				ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL RIESGO	BAJA
	SCTPSVR	Aplicación que maneja los paneles informativos del sistema.				ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL RIESGO	BAJA
	SIGET	Aplicación que maneja los turnos del personal de la vía y los técnicos de control.				ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL RIESGO	BAJA

						Medición - Riesgo Residual		
Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Control para Frecuencia	Control para Impacto	ZONA DE RIESGO	ESTRATEGIA DE ADMINISTRACIÓN DE RIESGOS	ulnerabilida
Antivirus	Antivirus Kaspersky – Anti Spam	Aplicación Antivirus	Avería de origen físico o lógico Errores de mantenimiento / actualización de programas (software) Vulnerabilidades de los programas (software)	Mantenimiento correctivo y preventivo, Politicas de seguridad	Soporte proveedor	ZONA DE RIESGO TOLERABLE	ASUMIR EL RIESGO, REDUCIR EL RIESGO	BAJA

Fuente: Autoría propia.

En el análisis de los aplicativos a la medida y al antivirus se evidencia una zona de riesgo tolerable y una vulnerabilidad baja después de aplicar controles.

Gráfica 34 análisis de riesgo a los Servidores.

B	C	D	E	L	M	Q	R	S
	Nombre					Medición - Riesgo Residual		
Servicio	Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Control para Frecuencia	Control para Impacto	ZONA DE RIESGO	ESTRATEGIA DE ADMINISTRACIÓN DE RIESGO	ulnerabilidad
Servidores	Server-TSM	IBM SYSTEM X350 XEON (Administrador de Tivoli)	Fuego Condiciones inadecuadas de temperatura o humedad Abuso de privilegios de acceso Avería de origen físico o lógico Suplantación de la identidad del usuario	Mantenimiento correctivo y preventivo, Politicas de seguridad, copias de seguridad, sistemas de detección, seguridad perimetral , antivirus.	PLAN DE CONTINUIDAD DEL NEGOCIO	ZONA DE RIESGO MODERADO	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	MEDIA
	Server - ALIM	HP PROLIANT BL380 G7 XEON (Soporta la carga de los archivos planos remitidos por los Alimentadores en la BD)						
	Server-apps	IBM HS22 (Type 7870) INTEL XEON (Aplicación WEB – CORDIS)						
	Server-Bd	IBM HS22 (Type 7870) INTEL XEON (BASES DE DATOS)						
	Server-Backup	IBM HS22 (Type 7870) INTEL XEON (BCK BASES DE DATOS)						
	Server-File	IBM HS22 (Type 7870) INTEL Xeonprocessor MP(ARCHIVO TODOS USUARIOS - SEUS)						
	Server-Clouster-1	IBM HS22 (Type 7870) INTEL Xeonprocessor MP(DNS, DHCP, ADFS CORREO EXCHANGE)						
	Server-Clouster-2	IBM HS22 (Type 7870) INTEL Xeon MP(DNS, DHCP, ADFS CORREO EXCHANGE)						
	Server-IIS64	IBM HS22 (Type 7870) INTEL Xeonprocessor MP(XIPE, SIGET(turnos), SLDF)						
	Server-IIS32	IBM HS22 (Type 7870) INTEL Xeonprocessor MP(ROYAL, KACTUS, PIGA)						
	Server- SEG	HP PROLIANT XEON (Arch. Temporales -Adm. Kaspersky)						
	Server- Alim2	IBM XEON (Archivos Posicionamiento Alimentadores)						
	Server - Test	HP PROLIANT XEON (AMBIENTE DE DESARROLLO)						

Fuente: Autoría propia.

En el análisis de riesgo a los Servidores se evidencia una zona de riesgo moderado y una vulnerabilidad media después de aplicar controles.

Gráfica 35 análisis de riesgo a las estaciones de trabajo y al servicio de Firewalls.

						Medición - Riesgo Residual		
Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Control para Frecuencia	Control para Impacto	ZONA DE RIESGO	ESTRATEGIA DE ADMINISTRACIÓN DE RIESGOS SUGERIDA	Vulnerabilidad
Estaciones de trabajo	AVANTE	CORE I3 - CORE I5 DD 500 GB - 1 TERA 6-8 GB RAM	Fuego Condiciones inadecuadas de temperatura o humedad Abuso de privilegios de acceso Avería de origen físico o lógico Suplantación de la identidad del usuario	correctivo y preventivo, Políticas de seguridad, copias de seguridad, sistemas de detección, seguridad perimetral , antivirus.	PLAN DE CONTINUIDAD DEL NEGOCIO	ZONA DE RIESGO MODERADO	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	MEDIA
	DELL	CORE 2 DUO - CORE 2 QUAD DD 160 - 500 GB 2-4 GB- RAM						
	HP	CORE 2 DUO - CORE I5 DD 80-500 GB 4-6 GB RAM						
	JANUS	CORE I3 - CORE I5 - CORE I7 DD 500 GB -1,5 TERAS RAM 4-8 GB						
	LENOVO	CORE I3 - CORE I5 DD 160 GB - 500 GB - RAM 2-8 GB						
	PCSMART	CORE I3						
Firewalls	DELL SonicWall NSA 3500	Seguridad Perimetral	Avería de origen físico o lógico Fuego Condiciones inadecuadas de temperatura o humedad	Mantenimiento correctivo y preventivo, Políticas de seguridad	Soporte proveedor	ZONA DE RIESGO MODERADO	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	MEDIA
	Dell SonicWALL Network Security Appliance NSA							
	Dell SonicWALLHigh Availability (HA) Unit NSA 3600							
Dispositivos de conectividad	ACCESS POINT		Avería de origen físico o lógico Fuego Condiciones inadecuadas de temperatura o humedad Fallo de servicios de comunicaciones Errores de [re-]encaminamiento	Mantenimiento correctivo y preventivo, Políticas de seguridad	Soporte proveedor	ZONA DE RIESGO TOLERABLE	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	BAJA
	MÓDEM							
	ROUTER							
	SWITCH							
Cuarto de comunicaciones		RACKS, CABLEADO, DISPOSITIVOS DE RED	Fuego Condiciones inadecuadas de temperatura o humedad Acceso no autorizado Desastres naturales Avería de origen físico o lógico	Mantenimiento correctivo y preventivo, Políticas de seguridad, seguridad perimetral, sistemas de detección	PLAN DE CONTINUIDAD DEL NEGOCIO	ZONA DE RIESGO TOLERABLE	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	BAJA

Fuente: Autoría propia.

En el análisis de riesgo a las estaciones de trabajo y al servicio de Firewalls se evidencia una zona de riesgo moderado y una vulnerabilidad media después de aplicar controles.

Gráfica 36 análisis de riesgo a las comunicaciones

						Medición - Riesgo Residual		
Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Control para Frecuencia	Control para Impacto	ZONA DE RIESGO	ESTRATEGIA DE ADMINISTRACIÓN DE RIESGOS SUGERIDA	Vulnerabilidad
Cableado Estructurado		CAT 6	Fuego Condiciones inadecuadas de temperatura o humedad Desastres naturales Avería de origen físico o lógico	Mantenimiento correctivo y preventivo	PLAN DE CONTINUIDAD DEL NEGOCIO	ZONA DE RIESGO TOLERABLE	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	BAJA
Medios de almacenamiento	CD-DVD USB CAMARAS		Alteración de la información Divulgación de la información Avería de origen físico o lógico	N/A	Políticas de seguridad	ZONA DE RIESGO TOLERABLE	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	BAJA
Dispositivos móviles	CELULARES TABLETS		Avería de origen físico o lógico	N/A	Políticas de seguridad	ZONA DE RIESGO TOLERABLE	REDUCIR EL RIESGO, EVITAR EL RIESGO,	BAJA
Impresoras			Avería de origen físico o lógico	Mantenimiento correctivo y preventivo	Soporte proveedor	ZONA DE RIESGO TOLERABLE	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O	BAJA
UPS, sistemas de detección, sistemas de enfriamiento, instalaciones eléctricas			Fuego Condiciones inadecuadas de temperatura o humedad Desastres naturales Avería de origen físico o lógico	Mantenimiento correctivo y preventivo, Políticas de seguridad, seguridad perimetral	PLAN DE CONTINUIDAD DEL NEGOCIO	ZONA DE RIESGO TOLERABLE	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	BAJA
Comunicaciones			Avería de origen físico o lógico Fallo de servicios de comunicaciones, Errores de (re-)encaminamiento Alteración de la información Divulgación de información Uso no previsto Interceptación de información (escucha)	Mantenimiento correctivo y preventivo, Políticas de seguridad, seguridad perimetral	PLAN DE CONTINUIDAD DEL NEGOCIO	ZONA DE RIESGO MODERADO	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	MEDIA

Fuente: Autoría propia.

En el análisis de riesgo a las comunicaciones se evidencia una zona de riesgo moderado y una vulnerabilidad media después de aplicar controles.

Gráfica 37 análisis de riesgo al servicio de Internet, Cloud computing, Intranet y Wifi Cuarto de comunicaciones y a las comunicaciones

						Medición - Riesgo Residual		
Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Control para Frecuencia	Control para Impacto	ZONA DE RIESGO	ESTRATEGIA DE ADMINISTRACIÓN DE RIESGOS SUGERIDA	Vulnerabilidad
Internet			Uso no previsto Fallo de servicios de comunicaciones Uso no previsto	Mantenimiento correctivo y preventivo, Políticas de seguridad,	PLAN DE CONTINUIDAD DEL NEGOCIO	ZONA DE RIESGO TOLERABLE	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O	BAJA
Cloud computing			Avería de origen físico o lógico Fallo de servicios de comunicaciones	Mantenimiento correctivo y preventivo, Políticas de seguridad,	PLAN DE CONTINUIDAD DEL NEGOCIO	ZONA DE RIESGO TOLERABLE	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O	BAJA
Intranet			Avería de origen físico o lógico Fallo de servicios de comunicaciones	Mantenimiento correctivo y preventivo, Políticas de seguridad,	PLAN DE CONTINUIDAD DEL NEGOCIO	ZONA DE RIESGO TOLERABLE	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O	BAJA
Wifi			Avería de origen físico o lógico Fallo de servicios de comunicaciones, Errores de (re-)encaminamiento Alteración de la información Divulgación de información Uso no previsto Interceptación de información (escucha)	Mantenimiento correctivo y preventivo, Políticas de seguridad, seguridad perimetral	PLAN DE CONTINUIDAD DEL NEGOCIO	ZONA DE RIESGO TOLERABLE	REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR O TRANSFERIR	BAJA

Fuente: Autoría propia.

Finalmente al realizar el análisis de riesgo al servicio de Internet, Cloud computing, Intranet y Wifi Cuarto de comunicaciones y a las comunicaciones se evidencia una zona de riesgo tolerable y una vulnerabilidad baja antes de aplicar controles.

Resultados:

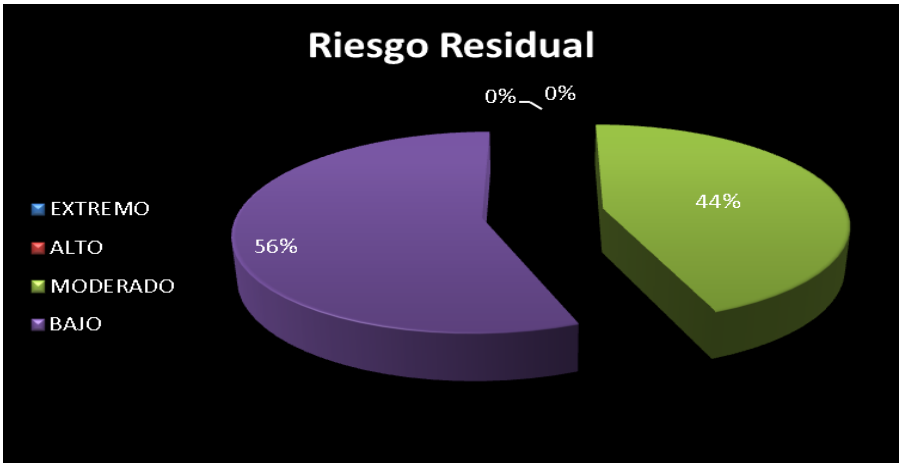
Riesgo Residual

Tabla 8 Calculo Riesgo Residual.

Riesgo Residual	Total
EXTREMO	0
ALTO	0
MODERADO	40
BAJO	51
TOTALES	**91**

Fuente: Autoría propia.

Gráfica 38 Riesgo Residual



Fuente: Autoría propia.

Una vez calculado el riesgo se toma una decisión sobre cómo se tratara el riesgo, esta decisión se toma sobre dos factores:

- Posible impacto si el riesgo se pone de manifiesto.
- Que tan frecuente suele suceder.

Las posibles estrategias que se toman para el tratamiento del riesgo son:

a. **Reducción del riesgo.** Se deben implementar controles apropiados para poder reducirlos al nivel que haya definido como aceptables. El control reduce el riesgo estimado así:

   - Reduciendo la posibilidad de que la vulnerabilidad sea explotada por la amenaza.

   - Reduciendo el posible impacto si el riesgo ocurriese, detectando eventos no deseados, reaccionando y recuperándose de ellos.

b. **Aceptación del riesgo.** Esta decisión se toma cuando no se encuentran controles para mitigar el riesgo, o la implantación de controles tiene un costo mayor que las consecuencias del riesgo.

c. **Transferencia del riesgo.** Esta decisión se adopta cuando para la compañía es difícil reducir o controlar el riesgo a un nivel aceptable. En esta circunstancia la transferencia a una tercera parte es más económica. Los mecanismos más utilizados son utilizar aseguradoras, utilizar terceros para el manejo de activos o procesos críticos, en la medida que tengan la capacidad de hacerlo.

d. **Evitar el riesgo.** Se refiere a cualquier acción orientada a cambiar las actividades, o la manera de desempeñar una actividad comercial en particular, para así evitar la presencia del riesgo. El riesgo se puede evitar si:

   - No desarrollar ciertas actividades comerciales.

   - Mover los activos de un área de riesgo.

   - Decidir no procesar información particularmente sensitiva.

e. **Tratamiento de los riesgos.** Se puede apreciar según el cuadro de valoración de riesgos que estos están en valores catastróficos por su probabilidad e impacto, pero la mayoría de estos pueden ser tratados definiendo controles y transfiriendo el riesgo.

Tabla 9 Tratamiento de riesgos.

RIESGO		TRATAMIENTO DEL RIESGO
Sistemas operativos		
R1	Usuarios sin restricciones	Definir controles
R2	Claves evidentes y compartidas	Aceptar y Definir controles
R3	Relación de confianza entre equipos	Definir controles
Software		
R4	Manuales de software y de procedimientos desactualizados o inexistentes	Definir controles
R5	Actualizaciones de seguridad (Parches)	Definir controles
Red		
R8	Alta disponibilidad	Definir controles
R9	Comunicaciones	Transferencia de riesgo (tercerizar servicio)
R10	Cloud computing	Transferencia de riesgo (tercerizar servicio)
Físico		
R11	Centro computo expuesto	Definir controles, transferencia de riesgo (vigilancia privada)
Personal		
R12	Usuarios sin restricciones	Establecer controles (control de acceso físico)
R13	Poca capacitación	Establecer controles (formación y concienciación), transferencia de riesgo (tercerizar servicio)

R14	Hacking	Establecer controles (cláusulas de confidencialidad), transferencia de riesgo (aseguradoras)

Fuente: Autoría propia.

A continuación se seleccionan solo los riesgos de mayor impacto (moderado, catastrófico) y probabilidad (media, alta) de ocurrencia, se identifica cuál es la causa que los origina y los recursos que se ven afectados (THU= talento humano, HW= hardware, SW= Software, ORG= toda la organización).

4.9.1.3. CAUSA DE LOS RIESGOS Y RECURSOS AFECTADOS

Sistemas operativos

R1.Usuarios sin restricciones; Probabilidad media Impacto catastrófico.

Se presenta por la falta de políticas que establezcan estándares desde el mismo comienzo de la implementación de los sistemas, y así evitar que cada una de las áreas solicite sus usuarios a la medida de sus requerimientos, el recurso que se ve afectado es toda la organización - ORG, ya que la consulta y manejo de información por funcionarios no autorizados puede convertirse en fuga de la misma (confidencialidad de los datos).

R2.Claves evidentes y compartidas; Probabilidad baja Impacto catastrófico.

No se implementaron estándares para fijar claves desde el inicio, permitiendo que las claves no tuvieran los mínimos requerimientos de seguridad. Por otro lado no se capacita a los funcionarios en el sentido de que las claves son personales y no se deben compartir.

R3.Relación de confianza entre equipos; Probabilidad media Impacto catastrófico.

Se presenta por la necesidad de compartir recursos entre usuarios de diferentes dominios. Se debe implementar solo aquellas relación que pasan a ser obligatorias en

el proceso administrativo. Se afecta todo la organización – ORG cuando los usuarios pasan a tener más privilegios de los requeridos

Software

R4.Manuales de software y de procedimientos desactualizados o inexistentes; Probabilidad media Impacto catastrófico.

- No se implanto un Sistema de Gestión de la Seguridad de la Información (SGSI), al no emplear una metodología PHVA (Planear, Hacer, Verificar y Actuar) que permita gestionar, salvaguardar los activos informáticos dentro de la organización, para protegerlos de los riesgos.

- No se realiza al interior de la empresa una sensibilización en las medidas de seguridad informática, los cuales incluyen estas actividades de actualización de manuales de software y procedimientos. Por lo tanto no se ha designado el personal que debe cumplir con estas actividades.

- Los profesionales de la oficina de informática no cuentan con el debido respaldo de la Dirección, para desarrollar las actividades relacionadas con la seguridad informática.

R5.Actualizaciones de seguridad (Parches); Probabilidad media Impacto catastrófico.

- Los sistemas deben tener disponibilidad permanente y cualquier actualización que se debe aplicar afectaría su disponibilidad.

- Las actualizaciones del software debe ser suministradas por los proveedores tanto del software a la medida como de software comercial, lo cual está sujeto a contratos, a los cuales no necesariamente dan continuidad ya que deben estar sujetos a licitaciones.

- Ahorro en costos de mantenimiento.

- Falla en los procedimientos o controles de actualización de código, lo que ocasiona que se sigan utilizando programas con defectos ya solucionados por el fabricante.

R8.Alta disponibilidad; Probabilidad media Impacto catastrófico.

La no implementación de equipos de alta disponibilidad y balanceo de cargas es primordial para un sistema de información, para lo cual es igualmente importante definir políticas y gestionar el riesgo generando procedimientos en casos de fallas o demora en cambios de servicios.

Se deben revisar los componentes que afectan el sistema de seguridad y que no se encuentra de manera redundante en caso de fallas, como son los firewall, servidores, copias de seguridad, etc. Además a los componentes ya existentes se les debe revisar las configuraciones y proceder a realizarles procedimientos de penetración de ser necesario.

R9.Comunicaciones; Probabilidad media Impacto catastrófico.

Es de vital importancia para la organización revisar detalladamente aspectos técnicos en las comunicaciones con el fin evitar errores, congestiones, sniffers, fallas físicas, configuraciones defectuosas, ataques DDos, etc.

Las políticas de seguridad frente a comunicaciones deben ser definidas con base a cifrado y manipulación de los sistemas informáticos.

Físico

R11. Centro computo expuesto; Probabilidad media Impacto catastrófico.

El acceso físico a los centros de cómputo debe tener parámetros y bitácoras de control, igualmente basándose en políticas de seguridad definidas en los estándares de seguridad de la información.

Personal

R12. Usuarios sin restricciones; Probabilidad media Impacto catastrófico.

El personal debe ser reglamentado frente accesos físicos y lógicos a los centros de cómputo, definiendo roles de acceso a servicios o equipos y servidores.

R13. Poca capacitación; Probabilidad media Impacto catastrófico.

La falta de capacitación es primordial por lo cual se deben generar directrices por parte de los directivos para la capacitación del personal, lo cual debe implementarse en políticas gerenciales.

R14. Hacking; Probabilidad media Impacto catastrófico.

La posibilidad de contar con ataques informáticos en una empresa depende de los sistemas de seguridad gestionados por lo cual generar políticas de seguridad para realizar pruebas de vulnerabilidad tanto externas con internas mitigan fuertemente la posibilidad de sufrir ataques informáticos de alto impacto.

A continuación se definen y describen las posibles soluciones de acuerdo al contexto de la organización, las soluciones o controles deben proponerse para cada riesgo y si un control se repite para dos o más riesgos, se definirá una sola vez el control que aparezca repetido.

4.9.1.4. SOLUCIONES Y/O CONTROLES DE LOS RIESGOS

Sistemas Operativos

R1.Usuarios sin restricciones; Probabilidad media Impacto catastrófico

Un usuario con todos los roles es un usuario sin restricciones, se deben establecer los diferentes perfiles de usuarios que ingresaran al sistema, inclusive los usuarios administradores, se debe restringir el alcance dentro de los sistemas y para ellos es necesario establecer claramente la separación de funciones.

R2.Claves evidentes y compartidas; Probabilidad baja Impacto catastrófico

Definir controles que obliguen a fijar claves seguras donde hay una cantidad mínima de caracteres, combinación de los mismos, tiempo de vida de las claves y la utilización

periódica de software que este evaluando su robustez. Controlar que los usuarios ingresen al sistema desde la terminal asignada a través de software o scripts.

R3.Relación de confianza entre equipos; Probabilidad media Impacto catastrófico.

Permanentemente se deben revisar los sistemas para que solo los usuarios autorizados estén utilizando la relación de confianza entre los equipos y de ser necesario bloquear los privilegios innecesarios. Sistemas de clúster y de alta disponibilidad hacer uso de esta característica por lo que se debe convivir con el riesgo.

Software

R4.Manuales de software y de procedimientos desactualizados o inexistentes

R5.Actualizaciones de seguridad (Parches)

Los riesgoss: “manuales de software y de procedimientos desactualizados o inexistentes” y “Actualizaciones de seguridad (Parches)”, pueden ser solventados con la implantación de controles.

Una vez se ha identificado los riegos de seguridad se ha tomado la decisión de hacer el tratamiento de los riesgos, se seleccionan los controles necesarios, los cuales se implementaran para asegurar que los riesgos se reduzcan a niveles aceptables. Dentro de los controles se incluyen políticas, procedimientos y directrices.

Los cambios o actualizaciones que se realizan a los sistemas para procesar la información deben realizarse con cuidado y cuando exista una razón válida para hacerlo, igualmente debe hacerse un control adecuado de los cambios realizados al sistema, ya que su inadecuada aplicación puede ser causa de vulnerabilidades e inestabilidad al sistema. De aquí la importancia de llevar un apropiado control de los cambios en mención.

Estos controles se pueden observar apreciar en los dominios de la norma ISO/IEC 27002:2005:

10. Gestión de comunicaciones y operaciones.

10.1 Procedimientos y responsabilidades operacionales

10.1.1 Procedimientos de operación documentados

10.1.2 Gestión del cambio

10.1.3 Segregación de los deberes

10.1.4 Separación de los medios de desarrollo, prueba y operación

10.2 Gestión de la entrega del servicio de terceros

10.2.1 Entrega del servicio

10.2.2 Monitoreo y revisión de los servicios de terceros

10.2.3 Manejo de cambios en los servicios de terceros

12. Adquisición, desarrollo y mantenimiento de sistemas de información.

12.1 Requerimientos de seguridad de los sistemas de información

12.1.1 Análisis y especificación de los requerimientos de seguridad

12.2 Procesamiento correcto en las aplicaciones

12.2.1 Validación de la input data

12.2.2 Control del procesamiento interno

12.2.3 Integridad del mensaje

12.2.4 Validación de la output data

12.4 Seguridad de los archivos del sistema

12.4.1 Control del software operacional

12.4.2 Protección de la data del sistema

12.4.3 Control de acceso al código fuente del programa

12.5 Seguridad en los procesos de desarrollo y soporte

12.5.1 Procedimientos del control del cambio

12.5.2 Revisión técnica de la aplicación después de cambios en el sistema

12.5.3 Restricciones sobre los cambios en los paquetes de software

12.5.4 Filtración de información

12.5.5 Desarrollo de software abastecido externamente

Red

R8.Alta disponibilidad; Probabilidad media Impacto catastrófico.

Se deben revisar los componentes que afectan el sistema de seguridad y que no se encuentra de manera redundante en caso de fallas, como son los firewall, servidores, copias de seguridad, etc. Además a los componentes ya existentes se les debe revisar las configuraciones y proceder a realizarles procedimientos de penetración de ser necesario.

R9.Comunicaciones; Probabilidad media Impacto catastrófico.

Los servicios que se prestan dependen de las comunicaciones, y estos deberían tener un alto porcentaje de confiablidad lo que conlleva a tener un contrato muy bien estructurado que nos brinde un excelente tiempo de respuesta a posibles fallos.

Físico

R11. Centro de computo expuesto; Probabilidad media Impacto catastrófico.

Como medida de control de acceso al centro de cómputo se implementara y un sistema biométrico que utilice huella, de tarjetas de aproximación y clave numérica que nos permitirá identificar el personal que ingresa y sale, además se implementara un sistema de ocho cámaras de vigilancia que apoyen el sistema biométrico.

Personal

R12. Usuarios sin restricciones; Probabilidad media Impacto catastrófico.

R13. Poca capacitación; Probabilidad media Impacto catastrófico.

R14. Hacking; Probabilidad media Impacto catastrófico.

Se deben generar políticas que incluyan restricciones a los usuarios en cuanto a instalación de software, control de descargas, manipulación de configuraciones, etc.

Se realizaran capacitaciones sobre seguridad informática a los funcionarios y contratistas de la entidad.

4.9.1.5. ESTUDIO DE IMPLEMENTACIÓN DE CONTROLES (COSTOS, TIEMPO Y PERSONAL)

Sistemas Operativos

R1.Usuarios sin restricciones; Probabilidad media Impacto catastrófico

Para identificar y establecer mecanismos en la creación de los usuarios y asignación de privilegios de tal manera que todos los privilegios no se concentren en un usuario, se implementara una herramienta que cruce los privilegios en cada uno de los sistemas, para ello se requiere inicialmente dos funcionarios que se encargaran del desarrollo, ejecución y mantenimiento de la herramienta que puede llegar a durar seis meses en su implementación, y tener un costo adicional para la empresa de $2’000.000 (dos millones de pesos) mensuales por funcionario en el área de seguridad.

R2.Claves evidentes y compartidas; Probabilidad baja Impacto catastrófico

Se deben implementar las políticas de claves seguras que traen todos los sistemas de información, para ello se encargaran todos los administradores de los servidores y a través de campañas en la intranet se informara de las nuevas políticas a los usuarios, el tiempo estimado para estabilizar el proceso de nuevas claves será de dos meses y no deberá generar costos adicionales.

R3.Relación de confianza entre equipos; Probabilidad media Impacto catastrófico.

Establecer un proceso de monitoreo y alerta para que los usuarios no trasgredan sus privilegios.

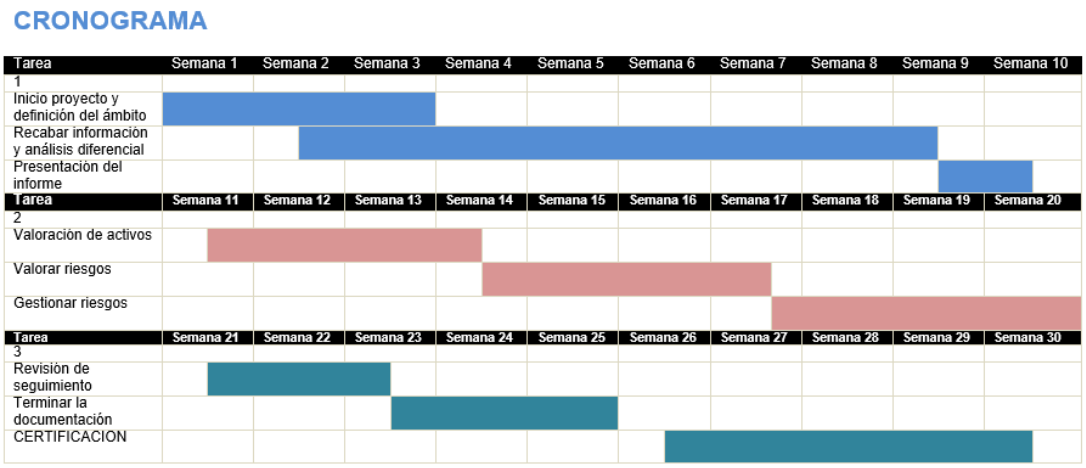
Software

R4.Manuales de software y de procedimientos desactualizados o inexistentes; Probabilidad media Impacto catastrófico.

R5.Actualizaciones de seguridad (Parches); Probabilidad media Impacto catastrófico.

A continuación se presenta un cronograma de actividades para la implantación de un SGSI, las actividades propia de la implantación de controles se involucran en la tarea 2, ya que no es posible definir los controles sin realizar las labores previas de valoración de activos y valoración de riesgos para realizar la gestión de los mismos.

Gráfica 39 Cronograma actividades Implementación SGSI.



Fuente: Autoría propia.

El costo promedio para la implementación y certificación ISO 27001 por parte de una entidad acreditadora se encuentra entre los COP4500000 y COP14000000.

La política de seguridad de información es de aplicación obligatoria para todo el personal de la empresa, independientemente del área y el nivel de atareas que desempeñe.

Las modificaciones de las políticas estarán en cabeza de la máxima autoridad que las aprueba.

El comité de seguridad de la información tendrá las siguientes funciones:

- Revisará y propondrá a la máxima autoridad del organismo la aprobación de la política de seguridad de la información y las funciones generales en materia de la seguridad de la información.

- Monitorear los cambios que sean más significativos en los riesgos y que afecten a los recursos de información frente a las amenazas más importantes.
- Entenderse de los incidentes relacionados con la seguridad de la información y supervisar las investigaciones.
- Tener la iniciativa para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área.
- Promover, difundir y apoyar la seguridad de la información dentro de la empresa y coordinar los procesos de continuidad del negocio dentro de la empresa.

El coordinador del comité de seguridad de la información será responsable de:

- Coordinar las actividades del comité de seguridad de la información.
- Impulsar la implementación y cumplimiento de la política de seguridad de la información.

El responsable de seguridad de la información:

- Cumple funciones relativas a la seguridad de los sistemas de información del organismo.

Los propietarios de la información y de los activos son responsables de:

- Clasificarla de acuerdo con el grado de sensibilidad y criticidad de la misma.
- Documentar y mantener actualidad la clasificación de la información.
- Definir los usuarios que deben tener permisos de acceso a la información de acuerdo a sus funciones y competencias.

Responsable del área de informática:

- Cumplir la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la empresa.

Red

R8.Alta disponibilidad; Probabilidad media Impacto catastrófico.

Ingeniero Especialista en seguridad para revisar configuraciones en los componentes que afectan el sistema de seguridad y que realice procedimientos de penetración (Ethical Hacking). $4.000.000 (cuatro millones de pesos / Mes).

R9.Comunicaciones; Probabilidad media Impacto catastrófico.

Profesional del área TICs que se encargue de revisar la confiablidad de los servicios de comunicaciones y que ejecute constante monitoreo a los tiempos de respuesta ante incidentes.

$3.200.000 (tres millones doscientos mil pesos / Mes).

Físico

R11. Centro computo expuesto; Probabilidad media Impacto catastrófico.

Compra e instalación y capacitación del sistema de cámaras y biométrico $6’000.000 (Seis millones de pesos)

Personal

R12. Usuarios sin restricciones; Probabilidad media Impacto catastrófico.

R13. Poca capacitación; Probabilidad media Impacto catastrófico.

R14. Hacking; Probabilidad media Impacto catastrófico.

Tabla 10 Cuadro resumen Implementación de controles.

	RIESGO	PROBABILIDAD			IMPACTO			TRATAMIENTO	CAUSA	RECURSOS AFECTADOS	SOLUCION	ESTUDIO DEL RIESGO		
		A	M	B	C	M	L					COSTOS MILLONES	TIEMPO EN MESES	PERSONAL
Sistemas operativos														
R1	Usuarios sin restricciones		X		X			Definir controles	Falta de politicas	ORG, SW	Implementacion Politicas Concienciacion	6	3	1 FUNCIONARIO 1 EXTERNO
R2	Claves evidentes y compartidas			X	X			Definir controles	Falta de politicas	ORG	Implementacion Politicas Concienciacion	0	2	1 FUNCIONARIO
R3	Relación de confianza entre equipos		X		X			Aceptarlo Definir controles	Recursos compartidos	ORG, SW	Monitoreo Permanente	0	1	1 FUNCIONARIO
Software														
R4	Manuales de software y de procedimientos desactualizados o inexistentes	X				X		Definir controles		ORG, SW	implementación y certificación ISO 27001	14	7	1 FUNCIONARIO 1 EXTERNO
R5	Actualizaciones de seguridad (Parches)		X		X			Definir controles		SW	implementación y certificación ISO 27001	0	4	1 FUNCIONARIO
Red														
R6	Falta de dispositivos de detección de intrusos		X		X			Definir controles	Sniffers, spoofing, phishing, port scanning, malware, etc.	THU, HW, SW, ORG	Implementacion Firewall, Proxy, IDS, IDPS, Honeypots, VPN	8	2	1 FUNCIONARIO 1 EXTERNOS
R7	Falta de herramientas de análisis de tráfico en la red		X		X			Definir controles	Errores, congestión, sniffers	THU, HW, SW, ORG	Wireshark, Tcpdump	8	2	1 FUNCIONARIO 1 EXTERNO
R8	Alta disponibilidad		X		X			Definir controles	Fallas físicas, Configuraciones defectuosas, ataques DDos	THU, HW, SW, ORG	Políticas de seguridad	4	1	EXTERNO
R9	Comunicaciones		X		X			Definir controles	Errores, congestión, sniffers, fallas físicas, configuraciones defectuosas, ataques DDos	THU, HW, SW, ORG	Políticas de seguridad	3,2	1	1 EXTERNO
Fisico														
R11	Centro computo expuesto		X		X			Definir controles, transferencia de riesgo (vigilancia privada)	Falta Personal Calificado en vigilancia	THU, HW, SW, ORG	Vigilancia privada	60	12	EXTERNO 7 X 24
Personal														
R12	Usuarios sin restricciones	X			X			Definir controles (control de acceso físico)	Falta Rastros y controsl ingresos centro computo	HW	Sistema biometrico	6	1	FUNCIONARIO
R13	Poca capacitación	X				X		Definir controles (formación y concienciación), transferencia de riesgo (terciarizar servicio)	Concienzacion	THU,ORG	Capacitacion permanente nuevas herramientas	10	1	EXTERNO
R14	Hacking	X			X			Definir controles (cláusulas de confidencialidad), transferencia de riesgo (aseguradoras)						

Fuente: Autoría propia.

5. POLÍTICAS DE SEGURIDAD TRANSMILENIO S.A.

Las políticas de seguridad de la información suministran herramientas de mejora en las conductas de los usuarios, lo que permite reducir los riesgos y responder a eventualidades, además asegura los activos de la empresa, establece una línea hacia la protección de la de la información frente a las diferentes amenazas, especifica sanciones en caso de infracción, ayuda a cumplir leyes, regulaciones, etc.

Los usuarios deben de concientizarse de la importancia de reconocer los conceptos básicos de la seguridad informática, lo cual requiere un fuerte trabajo de capacitación por parte de los administradores del área tecnológica, eso traerá como resultado muchos beneficios para la organización.

Dentro del proceso de diseño e implementación progresivo de la estrategia de seguridad de la información para TRANSMILENIO S.A., es preciso establecer un conjunto de políticas y procedimientos para la protección de los activos de la información.

Las políticas de seguridad suministran la base para la implementación de controles de seguridad que minimiza los riesgos y vulnerabilidades del sistema. La definición de las funciones y deberes

5.1. Seguridad de los recursos humanos:

El proceso de recursos humanos tiene establecido controles y medidas administrativas que permiten verificar no sólo la idoneidad del personal a contratar en un cargo específico, sino también su identidad, ética profesional y conducta.

Los términos y condiciones de empleo establecen los roles y responsabilidades a desempeñar en su cargo.

Al momento de incorporarse: como parte de los términos y condiciones iníciales de empleo, el empleado, cualquiera que sea, firma un compromiso de confidencialidad o no divulgación de la información relacionada con la actividad realizada en la Fundación.

La copia firmada del compromiso es custodiada por recursos humanos.

Durante el empleo o personal contratado: todos los empleados, y cuando sea pertinente los usuarios externos y los terceros que desempeñen funciones en la organización, recibirán una adecuada inducción de la seguridad del sistema de información.

Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general.

Funciones y deberes del personal

A continuación se relacionan las funciones y deberes para las personas que cuentan con acceso a los sistemas de información de la compañía, la definición de las funciones y deberes de los empleados tienen como objeto:

Preservar la seguridad de los sistemas de información y las redes de comunicación propiedad de la empresa o bajo su responsabilidad, contra el acceso o uso no autorizado, modificación indebida, destrucción, mal uso o hurto.

Resguardar la información perteneciente o proporcionada a la compañía, contra divulgaciones no permitidas o accidentales, alteración, destrucción o mal uso.

Con el fin de confirmar y verificar el cumplimiento de estos deberes, independiente de su cargo y responsabilidad, la compañía exige de manera general a cualquier trabajador cumplir con los siguientes aspectos:

5.2. Confidencialidad de la información

Proteger todo tipo de información de la organización, evitando el indebido uso o el envió externo no autorizado utilizando cualquier herramienta de comunicación.

Se deberá tener la mayor reserva, por tiempo indeterminado, sobre la información, documentos, métodos, contraseñas, programas y el resto de información a la que se posea acceso.

En caso de tratar con información confidencial, en cualquier tipo de soporte, se deberá entender que la posesión de esta es temporal, con obligación de secreto y sin que ello le concediera derecho alguno de posesión, titularidad o copia sobre esta. Inmediatamente después de la finalización de las tareas que hubieran originado el uso, debería devolverse a la entidad.

5.3. Propiedad Intelectual.

Está completamente prohibido en los Sistemas de Información de la compañía:

Utilizar aplicaciones informáticas sin la adecuada licencia. Los programas informáticos que pertenecen a la organización están protegidos por la propiedad intelectual y por lo tanto está prohibida su reproducción, alteración, transferencia o comunicación sin la debida autorización.

Utilizar, reproducir, modificar, ceder cualquier otro tipo de obra protegida por la propiedad intelectual sin la debida autorización.

5.4. Control de acceso físico y protección.

Las políticas en cuanto al acceso físico a las instalaciones de la organización que albergan los Sistemas de Información y los locales de tratamiento son las siguientes:

TRANSMILENIO S.A. deberá contar con los elementos de control acceso a los sistemas de información, entre los cuales podemos mencionar: Sistemas de video vigilancia en las áreas consideradas críticas, puertas de seguridad, control de ingreso con tarjetas inteligentes, sistemas de alarmas, software biométrico, sensores infrarrojos de movimiento, etc. Este esquema de seguridad debe almacenar un informe histórico de los accesos a los centros de cómputo, esto con el fin de brindar seguridad, tener control, llevar estadísticas y registros, etc. A continuación se establecen lineamientos para su implementación en la entidad.

Todo acceso a las ubicaciones de la infraestructura tecnológica, se realizara previo registro por un sistema de control de acceso físico o con autorización del personal responsable de la seguridad.

Todos los visitantes a la dirección de Tics, serán acompañados durante su estadía por un servidor de la entidad hasta que salga del área.

Siempre que un servidor de la entidad detecte un extraño dentro de las áreas restringidas de la dirección de Tics, inmediatamente deberá cuestionarlo acerca del propósito de su presencia en el área e informar al personal responsable de la seguridad.

5.5. Extracción de información.

Toda extracción de información de carácter personal en soportes informáticos o sistemas de información) deberá ser efectuada por el personal autorizado y se debe realizar bajo la autorización del autor del que provienen los datos.

En la extracción de datos de nivel alto / confidencial se deberán utilizar técnicas de cifrado o cualquier otra herramienta que impida el acceso o la manipulación durante su transferencia.

5.6. Incidentes

Todo trabajador de la compañía y terceras partes (contratistas, clientes, proveedores, etc.) tienen la obligación de informar cualquier incidente que se produzca y que esté relacionado con los sistemas de información o cualquier otro recurso informático de la organización.

La compañía utilizara un sistema de gestión de incidentes para comunicar, gestionar y resolver las incidencias de seguridad presentadas.

5.7. Uso adecuado de los recursos informáticos

Todos los recursos informáticos de la organización (datos, software, comunicaciones, etc.) están disponibles y deben ser utilizados únicamente para cumplir con los deberes laborales y con el propósito de gestionar sus actividades en la compañía. Por lo tanto, queda terminantemente prohibido cualquier uso diferente al señalado, a continuación ejemplos:

Utilizar equipos, dispositivos o aplicaciones que no estén definidos como parte del software y/o hardware contenidos en la compañía

Utilizar los sistemas de información o red corporativa para manipular contenidos prohibidos, inmorales o injuriosos y en general, sin provecho para los procesos de negocio de la empresa.

Introducir voluntariamente software, virus, malware o cualquier otro programa que tenga como objetivo causar daño en los recursos informáticos de la compañía.

Inhabilitar o desactivar el software antivirus y de protección de la maquina (pe. Firewall) y sus actualizaciones.

Intentar borrar, manipular, inutilizar los datos, software o cualquier otra información de la organización.

Pretender descubrir o descifrar passwords de acceso o penetrar cualquier otro dispositivo de seguridad que intermedie en los procesos telemáticos de la compañía.

5.8. Software

Llevar un inventario detallado y actualizado del software que maneja la organización.

Los encargados de la dirección de Tics deben asegurar que todos los equipos de la organización tengan instalado software legal.

Registrar los movimientos de compra, instalación o desinstalación de software en el inventario, además de contar con la respectiva autorización.

Los usuarios no han de instalar ni suprimir ningún tipo de software informático en su equipo.

Advertir a los usuarios las implicaciones legales que conlleva la instalación de software ilegal.

Verificar la compatibilidad del software y hardware para garantizar su óptimo funcionamiento.

La dirección de Tics (o en su defecto el encargado de su función) será responsable de delimitar el software de uso estandarizado en la compañía y de ejecutar las instalaciones en los equipos.

5.9. Hardware

Son aquellos elementos como computadores portátiles, módems, dispositivos de comunicación y computo propiedad de la entidad.

Es de vital importancia llevar un registro de los equipos de cómputo de la entidad.

- Identificar el responsable de cada equipo así como tener clara su localización.
- Conservar un inventario de los dispositivos de red en la compañía.
- El ingreso y salida del centro de cómputo o de la dirección de Tics de cualquier equipo deberá ser registrado en un formato elaborado para tal fin.
- Se debe actualizar y analizar al menos cada 6 meses los privilegios de acceso a las áreas protegidas.
- Se deben establecer diferentes puntos de control en las salidas para detectar la extracción no autorizada de equipos.
- Previo al retiro de cualquier equipo, es preciso contar con la autorización del área encargada.
- Todo tipo de equipo propiedad de TRANSMILENIO S.A. debe registrar su ingreso y salida y no debe ser sacado sin la autorización del responsable del área.
- Toda reubicación de (PCs, servidores, dispositivos de comunicación, etc.) debe tener una autorización previa.
- Los equipos de cómputo deben agregar identificadores electrónicos internos que permitan advertir su ingreso y salida de las instalaciones de la entidad.
- Los usuarios, en sus actividades laborales, deben hacer uso exclusivamente del hardware instalado en los equipos propiedad de la compañía y cuya función lo demande la función que desempeña.

- El usuario de ninguna manera accederá físicamente al interior de la maquina asignada para sus labores o que sea de propiedad de la organización, en este caso comunicara el incidente, a la dirección de Tics para que realice el procedimiento correspondiente.

5.10. Mantenimiento y protección de equipos

- Conservar los equipos según las recomendaciones del proveedor, en lo que refiere a configuraciones y especificaciones técnicas.
- Registrar en una bitácora los tipos de mantenimiento realizados a los equipos, las fechas, además de las medidas preventivas y correctivas que se hayan realizado.
- Proyectar la capacidad de los equipos a requerimientos futuros, esto con el fin de asegurar procesos y espacio de almacenamiento, es importante tener en cuenta velocidad de CPU, espacio de disco duro y memoria RAM.

5.11. Conexión a Internet

El servicio debe utilizarse única y exclusivamente para las tareas propias de la función desarrollada en Transmilenio y no debe utilizarse para ningún otro fin.

La autorización para acceder a Internet se podrá otorgar o bloquear de manera acorde con la función que los usuarios desempeñan en la empresa. Los accesos a Internet podrían estar regulados y vigilados por la dirección de Tics de la entidad.

El único navegador autorizado para el uso del servicio de Internet en Transmilenio es el asignado directamente por la dirección de Tics, el cual cumple con todos los requerimientos técnicos y de seguridad, evitando ataques de virus, spyware y otro tipo de software malicioso. Además este servicio tiene diferentes procesos de actualización que se aplican de manera periódica y segura.

Los servicios a los que un determinado usuario pueda acceder desde la Internet dependerán del rol que desempeña el usuario en Transmilenio y para los cuales este formal y expresamente autorizado.

5.11.1 Usos no aceptables del servicio

Este servicio no debe ser usado para:

- Envío o descarga de información masiva de gran tamaño que pueda congestionar la red.
- Envío, descarga, visualización de información con contenidos que atenten contra la integridad moral de las personas o instituciones.
- Acceso a páginas web, portales, sitios web y/o aplicaciones web que no hayan sido autorizadas por Transmilenio.
- Cualquier otro propósito diferente al considerado Uso aceptable del servicio.

5.12. Correo electrónico

Las normas referentes al correo electrónico son:

- Los usuarios autorizados para usar el servicio de correo electrónico son responsables de mantener un comportamiento ético y acorde a la ley y de evitar prácticas o usos que puedan comprometer la seguridad de la información de Transmilenio.
- El servicio debe ser empleado para servir a una finalidad operativa y administrativa en relación con Transmilenio. Todas las comunicaciones establecidas mediante este servicio, sus buzones y copias de seguridad se consideran de su propiedad y pueden ser revisadas por el administrador del servicio o cualquier instancia de vigilancia y control.

5.13. Seguridad de los equipos contra (virus, malware, troyanos, etc.)

Asegurar la protección de los equipos contra los virus y reconocer su clasificación en función de las múltiples características que estos poseen: su origen, técnicas utilizadas para infectar, tipos de ficheros infectados, daños causados, SO o plataforma atacada, etc.

- Los equipos deben tener instalado un antivirus totalmente funcional, que permita eliminar cualquier tipo de amenaza, además debe permitir una constante actualización.
- Contar con el soporte técnico especializado por parte de los distribuidores del software de seguridad.
- La dirección de Tics debe monitorear a través de una consola la operación del antivirus por parte de los usuarios y ante posibles manipulaciones crear alertas.
- Analizar detenidamente la posible la ejecución de software proveniente de fuentes desconocidas y poco confiables.
- Disponer de las últimas actualizaciones de software para los equipos de cómputo.
- Implementar controles para la detección y prevención de software malicioso.
- Instalar un firewall de software o hardware o alguna herramienta de seguridad que permita inspeccionar el estado de los puertos del sistema.

5.14. Plan de respaldo

Llevar la documentación de los procedimientos de operación: Si algún equipo tiene problemas en su normal funcionamiento, los registros deben permitir solucionar el inconveniente presentado, manejando tiempos de respuesta estimados según el caso.

La dirección de Tics vigilara el cumplimiento de las normas y políticas de seguridad de los activos tecnológicos de la compañía.

Monitorear y analizar cambios relacionados con las amenazas e incidentes más relevantes a los que están expuestos los recursos informáticos.

Respaldo de información fundamental

Obtener copias de seguridad actualizadas, en medios confiables que minimicen las posibilidades de un error.

- Tener un plan de recuperación ante un desastre que sea rápido y eficiente, para validar la confiabilidad del sistema de respaldo.

- Revisar los métodos y tiempos de respuesta de los backups para asegurar la calidad de la restauración.
- Procurar que las copias de respaldo sean automáticas por medio de un software que permita flexibilidad en su configuración.
- Definir el responsable de la revisión del proceso de copias, su almacenamiento y verificación de la exactitud y funcionalidad de la misma.

5.15. Sistema eléctrico

Contar con circuitos alternos independientes a cualquier conexión.

Disponer de un polo a tierra, conectado al sistema eléctrico de alimentación de las máquinas y la debida documentación de sus componentes.

Garantizar el suministro de energía eléctrica estable con el apoyo de sistemas de estabilización de voltaje, supresores de picos y unidades de potencia contra cortes inesperados (UPS).

Disponer de un plan de contingencia que establezca estrategias para enfrentar desastres.

5.16. Autenticación y seguridad en red

- Reconocer los inconvenientes relacionados con la conexión de red y sus servicios para establecer procedimientos que beneficien su utilización.
- Manejar de manera obligatoria la autenticación de usuarios para conexiones externas.
- Inspeccionar el acceso a los puertos abiertos con alguna herramienta de seguridad.
- Implementar la segmentación de la red para introducir controles y limitaciones en grupos específicos.

5.17. Sanciones Disciplinarias

La violación de alguna de estas políticas puede resultar en acciones disciplinarias que puede dar término de vinculación a los empleados y/o contratistas, suspensión o

expulsión sin excepción de la Institución. Adicionalmente los individuos están sujetos a perder el acceso a los privilegios, e iniciar un proceso civil y legal.

6. PROPUESTA PARA EL DESARROLLO DE UN SGSI EN EL ÁREA DE CONTRATACIÓN.

La propuesta de un SGSI - Sistema de Gestión de Seguridad de la información bajo la norma ISO 27001, no está orientada a despliegues de tecnología o infraestructura, esta maneja aspectos relacionados con la estructura de la seguridad de la información de la organización, esto supone una secuencia de acciones para establecer, implementar, operar, monitorear, revisar, mantener y la mejora continua del SGSI- Sistema de Gestión de Seguridad de la información.

El cuerpo de la norma se puede agrupar en 3 líneas:

SGSI - Sistema de Gestión de Seguridad de la información

Análisis y evaluación de riesgos

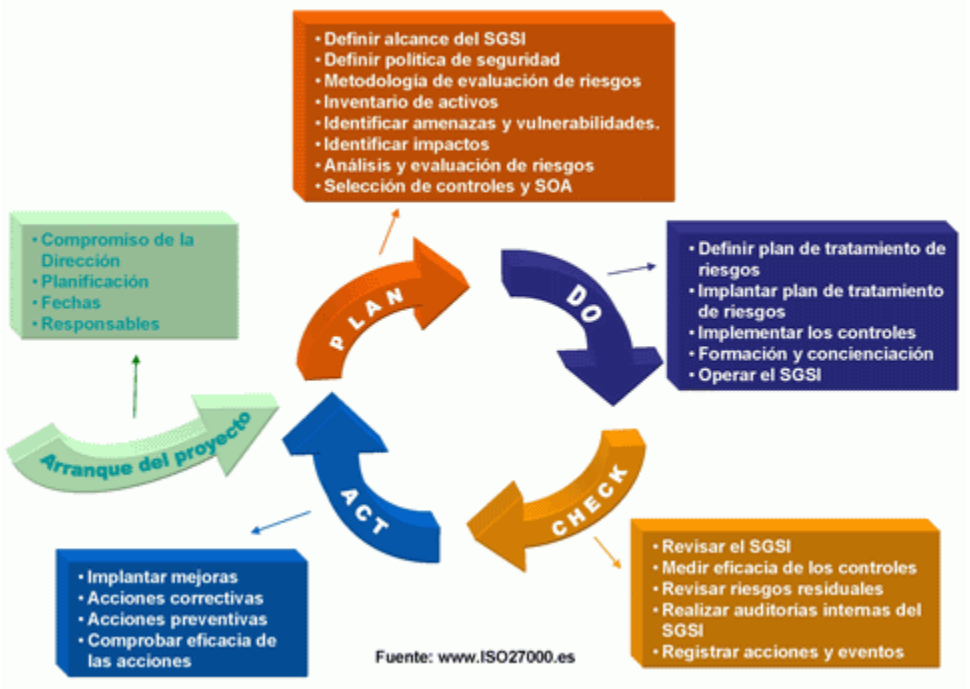
Controles

6.1. SGSI (SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN)

REQUERIMIENTOS GENERALES:

La entidad debe establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI - Sistema de Gestión de Seguridad de la información documentado que contextualice los riesgos de la organización dentro de las actividades propias del negocio. Para este propósito la norma se basa en el modelo PDCA (Planificar, Hacer, Verificar, Actuar).

Gráfica 40 Modelo PDCA aplicado a los procesos del SGSI.



Fuente: www.ISO27000.es

6.1.1.1. CONTROL DE DOCUMENTOS:

Los documentos solicitados por el SGS - Sistema de Gestión de Seguridad de la información I serán preservados y controlados. Un procedimiento documentado establecerá las acciones para:

- Aprobar y clasificar documentos y prioridades
- Revisar, actualizar y re aprobar documentos
- Asegurar que las versiones finales de los documentos estén disponibles para ser utilizadas.
- Asegurar la legibilidad de los documentos.
- Prevenir el uso no deseado de documentos obsoletos.

6.1.1.2. RESPONSABILIDAD DE LA ALTA GERENCIA:

La Alta Gerencia debe evidenciar su compromiso para establecer, implementar, operar, monitorear, revisar, mantener y mejorar del SGSI - Sistema de Gestión de Seguridad de la información por medio de:

- Establecer la política del SGSI - Sistema de Gestión de Seguridad de la información
- Establecer los objetivos del SGSI -Sistema de Gestión de Seguridad de la información
- Definir roles y responsabilidades
- Informar y concientizar a la compañía sobre la importancia y respaldo a los objetivos planteados en la política de seguridad, sus obligaciones legales y la necesidad de un mejoramiento continuo.
- Proporcionar los recursos suficientes para establecer, implementar, operar, monitorear, revisar, mantener y mejorar del SGSI.
- Definir los criterios de los niveles de riesgo y aceptación del mismo.
- Asegurar auditorías Internas al SGSI que lleven a la Alta Gerencia a su revisión constante al menos una vez al año.

6.1.1.3. FORMACIÓN, PREPARACIÓN Y COMPETENCIA:

La entidad debe asegurar que las personas con responsabilidades concretas en el SGSI -Sistema de Gestión de Seguridad de la información tengan las competencias suficientes para ejecutar las tareas requeridas, para esto debe proporcionar las herramientas y conocimiento necesario.

6.1.1.4. MEJORAS AL SGSI - Sistema de Gestión de Seguridad de la información

La entidad debe optimizar continuamente la eficiencia y eficacia del SGSI - Sistema de Gestión de Seguridad de la información por medio del uso de la política de seguridad de la información, sus objetivos, el resultado de las auditorias, la observación y monitoreo de sucesos, las medidas de prevención, corrección y su revisión.

6.1.1.5. MEDIDAS CORRECTIVAS:

La entidad ejecutara acciones para eliminar las causas que no estén de conformidad con lo querido por el SGSI - Sistema de Gestión de Seguridad de la información con el propósito de evitar su repetición, estas medidas correctivas deben ser documentadas.

6.2. ESTRUCTURA PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

La estructura contempla 3 niveles de compromiso,

- **Componente estratégico:** Alta Gerencia de TMSA establece reglas para la toma de decisiones.
- **Componente táctico:** Gerencia de la Integración define la metodología para lograr que las disposiciones del componente estratégico se concreten.
- **Componente Operativo:** Encargado de ejecutar la metodología propuesta por el nivel táctico.
- **Comité de Seguridad de la Información:** Debe estar incluido dentro del comité de gerencia y especificará reglas para la toma de decisiones óptimas en los aspectos relacionados del SGSI - Sistema de Gestión de Seguridad de la Información.

Esto con el fin de cumplir requisitos de la norma ISO 27001, en lo referente la responsabilidad de la dirección.

6.2.1.1. CONTROL INTERNO

La Ley 87 de 1993, señala que se entiende por control interno “el sistema integrado por el esquema de organización y el conjunto de los planes, métodos, principios, normas, procedimientos y mecanismos de verificación y evaluación adoptados por una organización, con el fin de procurar que todas las actividades, operaciones y actuaciones, así como la administración de la información y los recursos, se realicen de acuerdo con las normas constitucionales y legales vigentes dentro de las políticas trazadas por la dirección y en atención a las metas u objetivos previstos”. (Álvarez-correa, 2014)

6.2.1.2. OFICINA DE CONTROL INTERNO

Oficina que hace parte de la estructura formal de TRANSMILENIO S.A., dentro de un nivel directivo, con funciones específicas de asesoría y evaluación.

Su misión es realizar una evaluación objetiva e independiente del Sistema de Control Interno y la Gestión para asegurar el logro de los Objetivos Institucionales. (TRANSMILENIO S.A., 2014)

6.2.1.3. MECI

Decreto1599 de 2005 mediante el cual se adopta el Modelo Estándar de Control Interno MECI, con el fin de facilitar el desarrollo e implementación del Sistema de control interno en las organizaciones del Estado obligadas a cumplirlo.

- El modelo MECI detalla los lineamientos que se deben efectuar para el establecimiento del control interno en las entidades del estado, sin embargo no define una estructura organizacional para seguridad de la información.
- El modelo MECI define de manera clara que el control interno es una función que debe realizarse de manera independiente.
- El modelo MECI comprende la utilización de una metodología para gestionar riesgos que es compatible con diferentes normas entre ellas la ISO 27000. (Álvarez-correa, 2014).

6.2.1.4. DIRECCIÓN DE TICS

Un gran porcentaje de los controles tecnológicos adoptados para asegurar la información son gestionados por esta dirección, por este motivo la estructura de la seguridad de la información debe tener en cuenta esta área.

6.2.1.5. OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

En actualidad la compañía cuenta con un profesional con basta experticia en el área de seguridad de la información, entre sus conocimientos se evidencian:

1. Seguridad de la información.

2. Stack TCP/IP.

3. Implementación de SGC.

4. Implementación y auditorias de SGSI - Sistema de Gestión de la Seguridad de la Información

5. Gestión de Riesgos.

6. Informática Forense.

7. Ethical Hacking.

8. Arquitectura de software

9. Sistemas Operativos

10. Electricidad y Electrónica

6.3. CONCLUSIONES DE LA ESTRUCTURA ORGANIZACIONAL DE LA SEGURIDAD

- La organización de la seguridad de la información no demanda cambios estructurales en TRANSMILENIO S.A.
- Es preciso determinar en el comité de gerencia nuevas funciones estratégicas relacionadas con la seguridad de la información, con el objetivo de crear la figura del comité de seguridad de la información.
- La oficina de control debe fortalecer su campo de acción en cuantas auditorias informáticas con mínimo 2 ingenieros de sistemas expertos en el tema.
- La entidad debe contemplar en su plan de adquisiciones, un servicio de administración delegada de seguridad de la información, bajo la supervisión del Oficial de seguridad de la Información.
- Luego de ejecutar el análisis con base a la información recopilada, es posible establecer que la infraestructura tecnológica tiende a volverse más compleja debido a la evolución organizacional de TRANSMILENIO S.A., en función de eso los controles ya establecidos llegan a ser eficientes y deben seguir siendo optimizados, y alineados a una normativa que haya sido antes evidenciada como exitosa tal como lo es la norma ISO serie 27001.

- De manera general puede concluirse que se conservan actualmente controles que admiten mantener la información segura, no obstante estos controles pueden dejar de ser efectivos a medida que la infraestructura, y el volumen de la información van creciendo, razón por la cual es prudente mejorar los controles y alinearlos a la normativa ISO 27001 que permitirá fortalecer las políticas o controles existentes.
- Es necesario concretar un comité de seguridad de la información.
- De las responsabilidades detalladas por la norma ISO 27001, se concluye que se requieren los siguientes roles para la estructuración y organización de la seguridad, es necesario definir exactamente el responsable de cada actividad.

1) Rol de dirección: Responsabilidad en la toma de decisiones trascendentales del SGSI.
2) Rol de gestión administrativa: Responsable de tramitar procesos y recursos para conseguir que el SGSI cumpla con su función.
3) Rol de operación técnica: Responsabilidad de la operación técnica de los controles.
4) Rol de control y seguimiento: Se encargar de vigilar por el cumplimiento de las reglas que gobiernan el SGSI.
5) Rol de gestión de Incidentes: Encargado de efectuar un adecuado manejo.

- Por medio de la aplicación de esta norma se lograrán corregir u optimizar los controles existentes que dan origen a los siguientes problemas encontrados durante el desarrollo de este proyecto:
- Es necesario fortalecer los lineamientos de seguridad física que permitan atenuar riesgos de originen daños intencionados o no intencionados por parte de usuarios o terceros.
- Existen políticas documentadas las cuales no han sido revisadas ni difundidas desde el año 2010 con respecto al manejo o uso aceptable de los activos de información, ya sea hardware, software o datos.
- No se están empleando por completo los controles necesarios a fin de disminuir la difusión de malware en los equipos de cómputo, que pudieran incluso llegar a afectar servidores o repositorios de información.

- Existe evidencia de pérdida de equipos o dispositivos dentro de las oficinas de Transmilenio S.A., al ser sensibles a hurto.
- No existe un plan de contingencia documentado y divulgado a los empleados de la organización que permita garantizar la continuidad de las operaciones fundamentales en caso de un desastre.
- El factor humano, es habitualmente el punto más frágil en la seguridad de la información, se debe reforzar este aspecto a través de capacitaciones que permitan de una manera fácil a los usuarios reconocer los riesgos y amenazas asociados con el manejo de sistemas de información.
- Existe información que transita a través de diferentes medios de manera insegura, no existen al momento mecanismos de cifrado, si a través de estos medios se transfiriera información crítica se corre un alto riesgo de comprometer datos reservados y demás información sensible manipulada por los funcionarios de la compañía.
- Los controles de algunos servicios internos ofrecidos por la entidad, tales como SEUS, CORDIS, correo electrónico, etc. no son lo suficientemente robustos o funcionales, lo cual puede originar perdida de información, utilización excesiva de recursos como consecuencia de spam, perdida del servicio debido a errores en la base de datos y demás.

6.4. RECOMENDACIONES

- Generar un documento de seguridad que sea de fácil entendimiento para toda la organización y que se dé a conocer.
- Mantener de manera periódica el proceso de análisis de riesgos, y así evitar que nuevos ataques vulneren la información.
- Aunque se logre implementar un buen proceso de análisis de riesgos, de manera periódica mantener la contratación de organizaciones externas que permitan mayor objetividad en los aspectos relacionados con la seguridad de la información.
- Todos los riegos que se logren identificar se le deben medir su frecuencia, impacto y posibles soluciones.

- El área de Control Interno debe ser responsable de la auditoria interna de la seguridad de la información.
- El área de Tics debe estar vinculada directamente en la estructuración de la seguridad de la información.

Al evaluar el nivel actual de la seguridad de la información se evidencia que existen sistemas de información que son gestionados por terceros, es preciso implementar controles en el proceso de desarrollo de software, de acuerdo a las recomendaciones de la norma ISO 27001 es necesario destacar la función de gestión en el desarrollo del software.

El área de Tics debe ejecutar las labores de operación de la infraestructura IT, incluyendo gestión de los controles de seguridad. Con el objetivo de dar cumplimiento a recomendaciones de la norma ISO 27002 en lo referente a Procedimientos operacionales y responsabilidades.

6.4.1.1. EL SERVICIO DE INTERNET (COMUNICACIONES)

Los servicios que se prestan dependen de la comunicaciones, y estos deberían tener un alto porcentaje de confiablidad lo que conlleva a tener un contrato muy bien estructurado que brinde unos excelentes tiempos de respuesta ante posibles fallos. este debe estar ligado a un plan de continuidad del negocio que sirva para preparar a **TRANSMILENIO S.A.** en caso de incidentes prolongados causados por factores fuera de nuestro control (por ejemplo, desastres naturales, acontecimientos de origen humano), y para restaurar los servicios en la mayor medida posible con un mínimo tiempo de respuesta.

6.4.1.2. RED

Transmilenio S.A. debe contar con un firewall o dispositivo de seguridad perimetral de respaldo para la conexión a Internet o cuando sea inevitable para la conexión a otras redes en outsourcing o de terceros. Sus características se mencionan a continuación: Equipo activo de red para el soporte de las políticas y medidas de seguridad informática que se deban implementar. El hardware deberá tener capacidades y

funcionalidades para operar como una suite unificada de servicios de seguridad (Unified Threat Management - UTM), que cuente con facilidades, al menos de: IPS/IDS (Prevención y detección de intrusos), Antivirus, AntiSpam / Web Filtering (Filtrado de contenido y páginas de Internet), soporte de VPN, Firewall. La instalación y configuración del hardware será realizada acorde con la infraestructura de redes y equipos activos de red de TRANSMILENIO S.A..

6.4.1.3. SOFTWARE

Es recomendable adoptar políticas de actualización de software ya que debido esto se pueden presentar fallas en las aplicaciones que pueden llevar a la pérdida de información, ataques por vulnerabilidades de software, etc. Las actualizaciones no solo corrigen errores, si no también dan soporte a nuevas tecnologías, evitan vulnerabilidades de seguridad, corrigen en ocasiones problemas con el calentamiento de nuestros equipos o los mecanismos para interactuar con las memorias, pero sobre todas las cosas mantienen la estabilidad de nuestros sistemas operativos y software en general.

6.4.1.4. ALTA DISPONIBILIDAD

Se deben revisar los componentes que afectan el sistema de seguridad y que no se encuentran de manera redundante en caso de fallas, como son los firewall y además a los componentes ya existentes se les debe revisar las configuraciones y proceder a realizarles procedimientos de penetración de ser necesario.

6.4.1.5. SEGURIDAD FÍSICA

Se deben revisar los espacios físicos donde se encuentran los recursos informáticos y verificar que estos no se encuentran expuestos a problemas como interrupciones de energía, temperatura, incendios y otros de los cuales no podemos tener control pero que se pueden mitigar en caso de que sucedan como son las inundaciones, temblores y asonadas entre otros.

6.4.1.6. SISTEMAS DE RESPALDO

Los equipos no son infalibles y por lo tanto se debe contar con un esquema de respaldo que nos permita recuperarnos en caso de pérdida de información o algún daño del software o el hardware, estos esquemas se deben verificar para nos genere la confianza necesario en caso de que se presente el riesgo.

6.4.1.7. PERSONAL

La mejor manera de evitar que las personas que manejan los sistemas informáticos se conviertan en una vulnerabilidad es capacitándolos en todas las herramientas que manejan y enseñándoles los posibles riesgos en los que podrían caer.

7. BIBLIOGRAFÍA

ALIGNET. (2009). IT SECURITY. Retrieved from http://www.alignet.com/solucionesInfoSecurity.html

Allied Telesis. (2015a). AT-8000GS/24PoE. Retrieved from http://www.alliedtelesis.com/p-1884.html

Allied Telesis. (2015b). SwitchBlade® x908. Retrieved from http://www.alliedtelesis.sg/switches/sbx908

Álvarez-correa, S. P. (2014). CONTROL INTERNO PARA EL ESTADO COLOMBIANO MECI 2014 CONTROL INTERNO PARA EL ESTADO COLOMBIANO MECI 2014, 1–132. Retrieved from http://portal.dafp.gov.co/form/formularios.retrive_publicaciones?no=2162

BSIGROUP. (2015). ISO 22301: ISO 22301: Gestión de la Continuidad de Negocio. Retrieved from http://www.bsigroup.com/es-ES/ISO-22301-continuidad-de-negocio/

C3comunicaciones.es. (2014). Data Center: El Estándar TIA 942. Retrieved from http://www.c3comunicaciones.es/data-center-el-estandar-tia-942/

CATRIAN. (2014). Qué es un certificación TIER para un Centro de Datos. Retrieved from http://www.catrian.com/certificacion-tier/

firewalls-hardware.com. (2015). UTM, Gestión Unificada de Amenazas o Unified Threat Management. Retrieved from http://firewalls-hardware.com/unified-threat-management-gestion-unificada-amenazas-utm.asp

Insight Technology Solutions S.L. (2015). Kaspersky Enterprise Space Security. Retrieved from http://es.insight.com/es/shop/kaspersky/enterprise-space-security

INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Information security management systems — Overview and. (2014), *2014*.

ISO. (2015a). ISO 14000 - Environmental management. Retrieved from http://www.iso.org/iso/home/standards/management-standards/iso14000.htm

ISO. (2015b). ISO 27001 - Information security management. Retrieved from http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

ISO. (2015c). ISO 9000 - Quality management. Retrieved from http://www.iso.org/iso/iso_9000

ISO 27000.es. (2013). Portal de ISO 27001 en Español. Retrieved from http://www.iso27000.es

ISO/IEC. (2005). INTERNACIONAL ISO / IEC 27001. Retrieved from http://201.236.192.166/moodle/sgsi/iso_27001.pdf

LUNA MATAMOROS, B., ORTÍZ RODRÍGUEZ, R., & PAREDES ARTEAGA, J. (2011). *Sistema de Gestión de Seguridad de la Información en el Area de Recursos Humanos*. ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL.

SECOP. (2015). TMSA-MIN-30-2014. Retrieved from https://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=14-13-3153606

SONICWALL. (2011). NSA Series.

TRANSMILENIO S.A. MANUAL DEL SIG (2012). COLOMBIA. Retrieved from http://www.transmilenio.gov.co/?q=es/node/2558

TRANSMILENIO S.A. (2013a). MISIÓN. Retrieved from http://www.transmilenio.gov.co/es/articulos/mision

TRANSMILENIO S.A. (2013b). ORGANIGRAMA. Retrieved from http://www.transmilenio.gov.co/es/articulos/organigrama

TRANSMILENIO S.A. (2013c). VISIÓN. Retrieved from http://www.transmilenio.gov.co/es/articulos/vision

TRANSMILENIO S.A. (2014). ¿Quiénes Somos? Retrieved from http://www.transmilenio.gov.co/es/articulos/quienes-somos

TRANSMILENIO S.A. (2015). MAPA DE PROCESOS. Retrieved from http://www.transmilenio.gov.co/es/articulos/mapa-de-procesos

8. GLOSARIO

ATAQUE POR DENEGACIÓN DE SERVICIOS O ATAQUE DOS (DENIAL OF SERVICE): Está enfocado en causar que los servicios o recursos no estén disponibles para los usuarios autorizados, casi siempre provoca problemas de conexión a la red pues el ataque es generado mediante la saturación de puertos con flujo de información lo que provoca la sobrecarga del servidor, esta técnica es utilizada por crackers para tumbar servidores objetivo.

AUDITORÍA: es un análisis que vigila que las políticas de seguridad de la empresa sean cumplidas, además verifica que los privilegios de los usuarios sean apropiados de acuerdo con sus actividades.

BACKTRACK: Es una distribución de seguridad de Linux que incluye diferentes herramientas para pruebas de penetración estas permiten evaluar las vulnerabilidades de los sistemas de información por profesionales en seguridad informática.

BUG: fallas en la ejecución de un programa que desencadenan resultados inesperados.

CERTIFICADO DIGITAL: documento que permite identificar a una persona en internet, se utiliza en trámites con diferentes entidades que prestan servicios on line.

CLOUD COMPUTING: computación en la nube, informática en la nube, es un concepto de negocio que ofrece servicios a través de internet, esta tecnología permite almacenar en servidores de internet de manera permanente cualquier tipo de información.

CONFIDENCIALIDAD: Es la propiedad de la información que asegura el acceso solamente a las personas autorizadas. En la seguridad informática se centra en la protección de datos y en la información que es intercambiada entre el emisor y uno o más receptores.

CONTROL DE ACCESO: Es un mecanismo de protección de los recursos que componen un sistema, ya sea una red, una base de datos, o los recursos de hardware o software de una máquina, para la cual se dispondrá de un sistema operativo que

gestione el acceso a estos. El control de acceso se hace generalmente mediante listas lógicas de usuarios y contraseñas previamente establecidas por este o por los administradores del sistema.

COPYLEFT: se utiliza al practicar el derecho de autor y permite la libre distribución de copias y versiones modificadas de cualquier tipo de obra o trabajo creativo, respetando determinadas reglas.

COPYRIGHT: Es un conjunto de normas que reglamentan los derechos morales y patrimoniales que tienen los autores según la ley sobre sus creaciones para ser reproducidas y distribuidas.

DIRECTIVA DOD 5200.28 (EE.UU.): Pertenece al estándar TCSEC "criterios de evaluación de sistemas informáticos de confianza creado por el departamento de defensa de los EE.UU Llamado el libro naranja define los requerimientos de seguridad para sistemas de información automáticos, según el ministerio de defensa de EE.UU. este estándar es obsoleto y sugiere utilizar el CC (CommonCriteria) y el CEM.

DISPONIBILIDAD: Procura brindar el acceso a la información y a los sistemas mediante usuarios autorizados en el momento requerido. La disponibilidad pretende evitar interrupciones de servicios debido a varios motivos como fallos de hardware, cortes de energía, actualizaciones, etc.

ESTÁNDAR INTERNACIONAL ISO/IEC2702: Este Estándar va orientado a la seguridad de la información en las organizaciones, de modo que las posibilidades de ser afectados por robo, daño o pérdida de información se reduzcan al máximo.

FIREWALL: también llamado cortafuegos es un dispositivo diseñado para bloquear accesos no autorizados siguiendo normas establecidas, pueden ser implementados en hardware y software o combinados entre sí.

FULL TCP CONNECTION: técnica de penetración de escaneo de puertos que busca descubrir cuales están disponibles, esta técnica abre una conexión completa con el equipo con el modo de conexión normal, tiene una fiabilidad del 100% en los resultados, aunque es la que más rastros deja en el log del sistema remoto.

HIJACKING: es otra amenaza muy común en lo que respecta al control de acceso, esta técnica consiste en la interceptación y robo de una sesión de algún usuario para apropiarse de algún servicio o recurso prestado por la red o los medios que esta dispone.

HUELLAS DIGITALES: Permiten identificar a un individuo de manera exacta, por medio de un dispositivo que captura la huella digital y de un software que ejecuta la comprobación.

INGENIERA SOCIAL: Método basado en engaño y persuasión y habilidades sociales, para obtener información significativa. El principio que sustenta la ingeniería social es el que en cualquier sistema "los usuarios son el eslabón más débil".

INTEGRIDAD: Es la propiedad que busca evitar alteraciones no autorizadas en los datos. La integridad pretende mantener de una manera exacta los datos, evitando manipulaciones por personas o procesos no autorizados

JAMMING: es una de las más reconocidas amenazas en cuanto al control de acceso, esta técnica consiste en el bloqueo de un canal de comunicación con la intensión de impedir el flujo de información en la red, imposibilitando el acceso a los recursos de la misma.

KERBEROS: Es un protocolo de seguridad que trabaja con la autenticación de usuarios en un dominio, muy popular en ambientes Unix.

LEY DE INTIMIDAD DE 1974 (EE. UU.): establece prácticas que regulan el manejo de la información conservada en sistemas de registros de agencias federales para asegurar la integridad y seguridad de estos datos.

LOG DEL SISTEMA: es un registro de las actividades realizadas en un sistema, generalmente se guarda en un archivo de texto.

MIDDLEWARE: Software que asegura la comunicación transparente entre dispositivos distribuidos por todo el mundo, garantiza la calidad del servicio, la seguridad, etc.

NORMA CC (COMMON CRITERIA): Facilita un conjunto de metodologías para detallar e identificar requisitos funcionales de seguridad que debe cumplir un producto o sistema TI y las medidas de garantía aplicadas sobre los mismos, en sus diferentes fases del ciclo de vida.

OTP: Contraseñas de un solo uso, una de la principales soluciones de autenticación; los usuarios combinan su número de identificación (PIN) con un código que aparece en la pantalla, así se obtiene una contraseña única que es utilizada para comprobar su identidad.

PENETRACIÓN AL SISTEMA OPERATIVO: Técnica que busca vulnerabilidades al SO para penetrarlo.

SEGURIDAD: La seguridad de la información busca la protección de los principios básicos de confidencialidad, integridad y disponibilidad de la misma y de los sistemas involucrados en su tratamiento.

SEGURIDAD EXTERNA: está compuesta por seguridad física y la seguridad operacional, es la encargada de proteger el sistema contra intrusos y desastres.

SEGURIDAD FÍSICA: Su objetivo impedir la entrada de intrusos para esto se vale de algunos sistemas de identificación física (Sistemas de huellas, reconocimiento facial, etc.), los mecanismos de detección son de vital importancia (Detectores de humo, sensores de calor, etc.).

SEGURIDAD OPERACIONAL: Son las diferentes políticas y procedimientos que se han implementado en la organización por los administradores del área tecnológica.

SISTEMAS CLÚSTER DE COMPUTADORES: Son conjuntos de computadores construidos utilizando hardware común, están conectados por una red de alta velocidad y se comportan como si fuesen un solo ordenador más potente que los comunes.

SISTEMAS GRID COMPUTING: Utiliza todo tipo de recursos (Cómputo, almacenamiento y software específico), que no pertenecen a un control central, utiliza la computación distribuida en la cual los recursos soportan diferentes arquitecturas

están conectados por redes WAN, su objetivo es integrar el uso de ordenadores de alto rendimiento, redes y bases de datos.

SNIFFING: Técnica en la que se implementa un software o aplicación determinada para capturar las tramas que circulan por una red, mediante la escucha pasiva. La cantidad de tramas que puede obtener un sniffer depende de la topología de red.

DECLARACIÓN DE APLICABILIDAD: (SOA -Statement of Applicability-, en sus siglas inglesas): documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones (LUNA MATAMOROS, ORTÍZ RODRÍGUEZ, & PAREDES ARTEAGA, 2011).

SPOOFING: Es una técnica en la cual se obtiene información relevante a través de la suplantación de identidad, generalmente con fines maliciosos o de investigación. Este tipo de ataques se pueden clasificar en función de la tecnología utilizada. Entre ellos tenemos el IP spoofing (quizás el más conocido), ARP spoofing, DNS spoofing, Web spoofing o email spoofing.

VULNERABILIDAD: son debilidades que presentan los sistemas los cuales pueden ser aprovechados por un atacante para comprometer la integridad, disponibilidad o confidencialidad de la información.

WIRESHARK: es un software analizador de protocolos y paquetes de red (sniffer), se utiliza por administradores de red para realizar análisis del tráfico en un momento determinado y solucionar problemas en una red de datos como errores, congestión, etc. Además captura cookies y passwords, que es el fin del presente trabajo.